Module: Renforcement des Acquis 1

Arithmétiques dans $\mathbb{Z}$ - Structures algébriques

Mohamed Talbi   Mohammed Talbi

Centre régional des métiers de l'éducation et de la formation de l'oriental
Oujda, Maroc

Département de mathématiques

2021-2022



Chapitre 1 : Arithmétiques dans $\mathbb{Z}$

Définition

Soient a un entier relatif non nul et b un entier relatif. On dit que b est divisible par a dans $\mathbb{Z}$ ou que a divise b dans $\mathbb{Z}$ et on écrit $a \mid b$, s'il existe un entier relatif k tel que $b = ka$.
Dans ce cas, on dit que b est un multiple de a ou que a est un diviseur de b.
L'ensemble des diviseurs de b est noté par $D(b)$. Dans le cas contraire on écrit $a \nmid b$.

Définition

Soient a un entier relatif non nul et b un entier relatif. On dit que b est divisible par a dans $\mathbb{Z}$ ou que a divise b dans $\mathbb{Z}$ et on écrit $a \mid b$, s'il existe un entier relatif k tel que $b = ka$.
Dans ce cas, on dit que b est un multiple de a ou que a est un diviseur de b.
L'ensemble des diviseurs de b est noté par $D(b)$. Dans le cas contraire on écrit $a \nmid b$.

Exemple

- $2 \mid 6$ *car* $6 = 3 \times 2$ *et on a* $D(6) = \{-6; -3; -2; -1; 1; 2; 3; 6\}$.
- $2 \nmid 7$ *car* $(\nexists k \in \mathbb{Z}) : 7 = 2k$.

Lemme

Si $a \mid b$ *et* $b \neq 0$*, alors* $|a| \leq |b|$*. Ainsi tout entier non nul admet un nombre fini de diviseurs.*

Lemme

Si $a \mid b$ *et* $b \neq 0$, *alors* $|a| \leq |b|$. *Ainsi tout entier non nul admet un nombre fini de diviseurs.*

Preuve.

On a

$$\begin{aligned} a \mid b \text{ et } b \neq 0 &\Longrightarrow (\exists k \in \mathbb{Z}) : b = ka \text{ et } k \neq 0 \\ &\Longrightarrow (\exists k \in \mathbb{Z}) : |b| = |k| \cdot |a| \text{ et } |k| \geq 1 \\ &\Longrightarrow |a| \leq |b|. \end{aligned}$$

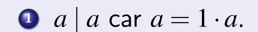


Propriétés

Soient a, b et c trois entiers relatifs, alors :

1. $a \mid a$ *(avec $a \neq 0$).*
2. *Si $a \mid b$ et $b \mid c$, alors $a \mid c$.*
3. *Si $a \mid b$ et $b \mid a$, alors $|a| = |b|$ c'est-à-dire $a = \pm b$.*
4. *Si $a \mid b$ et $c \mid d$, alors $ac \mid bd$.*
5. *Si $a \mid b$ et $a \mid c$, alors $a \mid mb + nc, \forall (m,n) \in \mathbb{Z}^2$.*
6. *Si $a \mid b$, alors $(\forall c \in \mathbb{Z}^*)$; $ac \mid bc$.*

Preuve.



1. $a \mid a$ car $a = 1 \cdot a$.

Preuve.

1. $a \mid a$ car $a = 1 \cdot a$.
2. On a $a \mid b$, alors $(\exists k \in \mathbb{Z}) : b = ka$, et $b \mid c$, alors $(\exists k' \in \mathbb{Z}) : c = k'b$, ainsi $c = (kk')a$, ce qui donne que $a \mid c$.

Preuve.

1. $a \mid a$ car $a = 1 \cdot a$.
2. On a $a \mid b$, alors $(\exists k \in \mathbb{Z}) : b = ka$, et $b \mid c$, alors $(\exists k' \in \mathbb{Z}) : c = k'b$, ainsi $c = (kk')a$, ce qui donne que $a \mid c$.
3. Si $a \mid b$ et $b \mid a$, alors $|a| \leq |b|$ et $|b| \leq |a|$, ainsi $|a| = |b|$ c'est-à-dire $a = \pm b$.

Preuve.

1. $a \mid a$ car $a = 1 \cdot a$.
2. On a $a \mid b$, alors $(\exists k \in \mathbb{Z}) : b = ka$, et $b \mid c$, alors $(\exists k' \in \mathbb{Z}) : c = k'b$, ainsi $c = (kk')a$, ce qui donne que $a \mid c$.
3. Si $a \mid b$ et $b \mid a$, alors $|a| \leq |b|$ et $|b| \leq |a|$, ainsi $|a| = |b|$ c'est-à-dire $a = \pm b$.
4. On a $a \mid b$, alors $(\exists k \in \mathbb{Z}) : b = ka$, et on a $c \mid d$, alors $(\exists k' \in \mathbb{Z}) : d = k'c$, donc $bd = (ka) \cdot (k'c) = (kk') \cdot (ac)$, c'est-à-dire $ac \mid bd$.

Preuve.

1. $a \mid a$ car $a = 1 \cdot a$.
2. On a $a \mid b$, alors $(\exists k \in \mathbb{Z}) : b = ka$, et $b \mid c$, alors $(\exists k' \in \mathbb{Z}) : c = k'b$, ainsi $c = (kk')a$, ce qui donne que $a \mid c$.
3. Si $a \mid b$ et $b \mid a$, alors $|a| \leq |b|$ et $|b| \leq |a|$, ainsi $|a| = |b|$ c'est-à-dire $a = \pm b$.
4. On a $a \mid b$, alors $(\exists k \in \mathbb{Z}) : b = ka$, et on a $c \mid d$, alors $(\exists k' \in \mathbb{Z}) : d = k'c$, donc $bd = (ka) \cdot (k'c) = (kk') \cdot (ac)$, c'est-à-dire $ac \mid bd$.
5. On a $a \mid b$ et $a \mid c$, alors $(\exists k \in \mathbb{Z}) : b = ka$ et $(\exists k' \in \mathbb{Z}) : c = k'a$, ainsi $(\forall (m,n) \in \mathbb{Z}^2$, $(\exists (k,k') \in \mathbb{Z}^2) : mb + nc = (mk)a + (nk')a = (mk + nk')a$, ce qui donne que $a \mid mb + nc, (\forall (m,n) \in \mathbb{Z}^2)$.
6. Trivial.



Théorème

Soient a *et* b *deux entiers relatifs, avec* $b > 0$. *Il existe un couple unique* $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ *vérifiant* $a = bq + r$ *et* $0 \leq r < b$.
L'entier q *s'appelle le quotient et l'entier* r *s'appelle le reste de la division euclidienne de* a *par* b.

Preuve.

Soit $A = \{a - bk \mid k \in \mathbb{Z}\} \cap \mathbb{N}$.

- L'ensemble A est non vide,

Preuve.

Soit $A = \{a - bk \mid k \in \mathbb{Z}\} \cap \mathbb{N}$.

- L'ensemble A est non vide, car si $a \geq 0$, alors $a \in A$ en prenant $k = 0$ et si $a < 0$, alors $a(1-b) \in A$ en prenant $k = a$.

Preuve.

Soit $A = \{a - bk \mid k \in \mathbb{Z}\} \cap \mathbb{N}$.

- L'ensemble A est non vide, car si $a \geq 0$, alors $a \in A$ en prenant $k = 0$ et si $a < 0$, alors $a(1-b) \in A$ en prenant $k = a$.
- D'après la propriété fondamentale de $\mathbb{N}$, l'ensemble A admet un plus petit élément qu'on note par r, il existe donc $q \in \mathbb{Z}$ tel que $r = a - bq$.

Preuve.

Soit $A = \{a - bk \mid k \in \mathbb{Z}\} \cap \mathbb{N}$.

- L'ensemble A est non vide, car si $a \geq 0$, alors $a \in A$ en prenant $k = 0$ et si $a < 0$, alors $a(1-b) \in A$ en prenant $k = a$.
- D'après la propriété fondamentale de $\mathbb{N}$, l'ensemble A admet un plus petit élément qu'on note par r, il existe donc $q \in \mathbb{Z}$ tel que $r = a - bq$.

Supposons que $r \geq b$, on aura alors

$$0 \leq r - b = a - bq - b = a - b(q+a) \in A,$$

ainsi on a $0 \leq r - b < r$, ce qui contredit le fait que r est le plus petit élément de A, par conséquence $0 \leq r < b$ et $a = bq + r$.
Supposons qu'il existe un autre couple $(q', r') \in \mathbb{Z} \times \mathbb{Z}$ vérifiant

$$a = bq' + r' \text{ et } 0 \leq r' < b.$$

Si $q \neq q'$, alors on peut supposer que $q - q' \geq 1$, donc $b \leq b(q-q') = r' - r \leq r'$, ce qui contredit le fait que $r' < b$. Ainsi $q = q'$ et par suite $r = r'$. □

Théorème (Division euclidienne étendue)

Soient a et b deux entiers relatifs, avec $b \neq 0$. Il existe un couple unique $(q,r) \in \mathbb{Z} \times \mathbb{Z}$ vérifiant $a = bq + r$ et $0 \leq r < |b|$.

Théorème (Division euclidienne étendue)

Soient a et b deux entiers relatifs, avec $b \neq 0$. Il existe un couple unique $(q,r) \in \mathbb{Z} \times \mathbb{Z}$ vérifiant $a = bq + r$ et $0 \leq r < |b|$.

Preuve.

Si $b < 0$, on effectue la division euclidienne de a par $-b$, donc il existe un couple unique $(q',r) \in \mathbb{Z}^2$ vérifiant $a = (-b)q' + r$ et $0 \leq r < -b$ c'est-à-dire $a = b(-q') + r$ et $0 \leq r < -b$.
Prenons $q = -q'$, donc $a = bq + r$ et $0 \leq r < |b|$. □

Exemple

- *La division euclidienne de* 18 *par* 6 *est*

Exemple

- *La division euclidienne de* 18 *par* 6 *est*

$$18 = 6 \times 3$$

(le quotient est 3 *et le reste est* 0*).*

- *La division euclidienne de* 15 *par* 2 *est*

Exemple

- *La division euclidienne de* 18 *par* 6 *est*

$$18 = 6 \times 3$$

  (le quotient est 3 *et le reste est* 0*).*

- *La division euclidienne de* 15 *par* 2 *est*

$$15 = 2 \times 7 + 1$$

  (le quotient est 7 *et le reste est* 1*).*

- *La division euclidienne de* -55 *par* 3 *est*

Exemple

- *La division euclidienne de* 18 *par* 6 *est*

$$18 = 6 \times 3$$

(le quotient est 3 *et le reste est* 0*).*

- *La division euclidienne de* 15 *par* 2 *est*

$$15 = 2 \times 7 + 1$$

(le quotient est 7 *et le reste est* 1*).*

- *La division euclidienne de* -55 *par* 3 *est*

$$-55 = 3 \times (-19) + 2$$

(le quotient est (-19) *et le reste est* 2*).*

Définition

On dit qu'un entier relatif p *est premier si* p *a exactement quatre diviseurs dans* $\mathbb{Z}$*, à savoir* $-p,\ p,\ -1$ *et* 1 *c'est-à-dire* $D(p) = \{-p;\ p;\ -1;\ 1\}$.

Définition

On dit qu'un entier relatif p est premier si p a exactement quatre diviseurs dans $\mathbb{Z}$, à savoir $-p,\ p,\ -1$ et 1 c'est-à-dire $D(p) = \{-p;\ p;\ -1;\ 1\}$.

Remarque

Si p est premier, alors $-p$ est aussi premier. Pour ceci, on s'interesse seulement aux nombres premiers positifs $(\in \mathbb{N})$ et on note par $\mathbb{P}$ l'ensemble de ces nombres premiers.

Pour que $p \in \mathbb{N}$ sera dans $\mathbb{P}$ il faut et il suffit que p a exactement deux diviseurs dans $\mathbb{N}$, à savoir 1 et p lui même.

Dans toute la suite

un nombre premier veut dire un nombre premier positif.

Exemple

1. $2,\ 3,\ 5,\ 7,\ 11,\ 13\ldots$ *sont des nombres premiers.*
2. 14 *n'est pas un nombre premier car* 14 *a plus de deux diviseurs dans* $\mathbb{N}$.
3. 1 *n'est pas un nombre premier car* 1 *a un seul diviseur dans* $\mathbb{N}$, *à savoir* 1.
4. *On peut tester la primalité d'un entier naturel* n *en utilisant le logiciel* $PARI$, *par la commande "isprime" :*
   - $isprime(n) = 1$ *c'est-à-dire* $n \in \mathbb{P}$.
   - $isprime(n) = 0$ *c'est-à-dire* $n \notin \mathbb{P}$.
5. *On peut connaître les* n *premiers nombres premiers positifs en utilisant le logiciel* $PARI$, *par la commande "*$primes(n)$*" :*
   - $primes(7)$ *donne les* 7 *premiers nombres premiers positifs, à savoir :* $2,\ 3,\ 5,\ 7,\ 11,\ 13$ *et* 17.

Proposition

Soit n un entier relatif tel que $|n| \geq 2$, alors le plus petit diviseur supérieur ou égal à 2 de n est un nombre premier.

Proposition

Soit n un entier relatif tel que $|n| \geq 2$, alors le plus petit diviseur supérieur ou égal à 2 de n est un nombre premier.

Preuve.

Soit $n \in \mathbb{Z}$ tel que $|n| \geq 2$, alors l'ensemble A des diviseurs positifs de n supérieur ou égal à 2 est une partie non vide de $\mathbb{N}$ (il contient au moins $|n|$), alors il admet un plus petit élément qu'on notera par p. Soit $q \geq 2$ un diviseur de p, alors il existe $k \in \mathbb{N}$ tel que $p = kq \geq q$. Comme $q \mid p$ et $p \mid n$, alors $q \mid n$ et $q \geq 2$, ainsi $q \in A$ et comme p est le plus petit élément de A, alors $q = p$, par suite p est un nombre premier. □

Remarque (Test de primalité)

Soit n *un entier positif non premier, alors* n *possède un diviseur premier inférieur ou égal à* $\sqrt{n}$*. Donc si aucun nombre premier inférieur ou égal à* $\sqrt{n}$ *ne divise* n*, alors* n *est un nombre premier.*

Remarque (Test de primalité)

Soit n *un entier positif non premier, alors* n *possède un diviseur premier inférieur ou égal à* $\sqrt{n}$*. Donc si aucun nombre premier inférieur ou égal à* $\sqrt{n}$ *ne divise* n*, alors* n *est un nombre premier.*
En effet, soit $n \in \mathbb{N}^*$ *non premier et* p *son plus petit diviseur supérieur ou égal à* 2*, alors* p *est premier. Comme* $p \mid n$*, alors il existe* $k \in \mathbb{N}$ *tel que* $n = pk$*. Comme* n *n'est pas premier, alors* $k > 1$ *et puisque* $k \mid n$*, alors* $p \leq k$*. Ainsi* $n = pk \geq p^2$*, ce qui donne que* $p \leq \sqrt{n}$*.*

Théorème

L'ensemble des nombres premiers $\mathbb{P}$ *est infini.*

Théorème

L'ensemble des nombres premiers $\mathbb{P}$ est infini.

Preuve.

Supposons que l'ensemble $\mathbb{P}$ est fini.

Théorème

L'ensemble des nombres premiers $\mathbb{P}$ est infini.

Preuve.

Supposons que l'ensemble $\mathbb{P}$ est fini.
On a $\mathbb{P} \neq \emptyset$ (car $2 \in \mathbb{P}$).

Théorème

L'ensemble des nombres premiers $\mathbb{P}$ est infini.

Preuve.

Supposons que l'ensemble $\mathbb{P}$ est fini.
On a $\mathbb{P} \neq \emptyset$ (car $2 \in \mathbb{P}$). Soit p le plus grand élément de $\mathbb{P}$ et soit $m = p! + 1$.

Théorème

L'ensemble des nombres premiers $\mathbb{P}$ est infini.

Preuve.

Supposons que l'ensemble $\mathbb{P}$ est fini.
On a $\mathbb{P} \neq \emptyset$ (car $2 \in \mathbb{P}$). Soit p le plus grand élément de $\mathbb{P}$ et soit $m = p! + 1$. On a $m > p$, donc $m \notin \mathbb{P}$, il possède donc un diviseur premier qu'on notera par q.
Comme p est le plus grand élément de $\mathbb{P}$, alors $q \leq p$, ainsi $q \mid p!$ et comme $q \mid m$, alors $q \mid m - p! = 1$, ce qui donne que $q = 1$, ce qui contredit le fait que q est un nombre premier. Ainsi l'ensemble $\mathbb{P}$ est infini. □

Définition

Soient a et b deux entiers relatifs non tous les deux nuls. Un entier $d \geq 1$ est dit le plus grand commun diviseur de a et b, qu'on le note par $\operatorname{pgcd}(a,b)$ ou $a \wedge b$, si les deux conditions suivantes sont satisfaites :

- *d est un diviseur commun de a et b* c'est-à-dire $d \in D(a) \cap D(b)$;
- *Tout diviseur commun de a et b divise d* c'est-à-dire $\forall n \in D(a) \cap D(b),\ n \mid d$.

Définition

Soient a *et* b *deux entiers relatifs non tous les deux nuls. Un entier* $d \geq 1$ *est dit le plus grand commun diviseur de* a *et* b*, qu'on le note par* $\mathrm{pgcd}(a,b)$ *ou* $a \wedge b$*, si les deux conditions suivantes sont satisfaites :*

- d *est un diviseur commun de* a *et* b *c'est-à-dire* $d \in D(a) \cap D(b)$ *;*
- *Tout diviseur commun de* a *et* b *divise* d *c'est-à-dire* $\forall n \in D(a) \cap D(b),\ n \mid d.$

Exemple

- $(-12) \wedge 4 =$

Définition

Soient a et b deux entiers relatifs non tous les deux nuls. Un entier $d \geq 1$ est dit le plus grand commun diviseur de a et b, qu'on le note par $\mathrm{pgcd}(a,b)$ ou $a \wedge b$, si les deux conditions suivantes sont satisfaites :

- *d est un diviseur commun de a et b c'est-à-dire $d \in D(a) \cap D(b)$;*
- *Tout diviseur commun de a et b divise d c'est-à-dire $\forall n \in D(a) \cap D(b),\ n \mid d$.*

Exemple

- $(-12) \wedge 4 = 4.$
- $18 \wedge 27 =$

Définition

Soient a *et* b *deux entiers relatifs non tous les deux nuls. Un entier* $d \geq 1$ *est dit le plus grand commun diviseur de* a *et* b*, qu'on le note par* $\text{pgcd}(a,b)$ *ou* $a \wedge b$*, si les deux conditions suivantes sont satisfaites :*

- d *est un diviseur commun de* a *et* b *c'est-à-dire* $d \in D(a) \cap D(b)$ *;*
- *Tout diviseur commun de* a *et* b *divise* d *c'est-à-dire* $\forall n \in D(a) \cap D(b),\ n \mid d$*.*

Exemple

- $(-12) \wedge 4 = 4$.
- $18 \wedge 27 = 9$.
- $8 \wedge 5 =$

Définition

Soient a et b deux entiers relatifs non tous les deux nuls. Un entier $d \geq 1$ est dit le plus grand commun diviseur de a et b, qu'on le note par $\mathrm{pgcd}(a,b)$ ou $a \wedge b$, si les deux conditions suivantes sont satisfaites :

- *d est un diviseur commun de a et b c'est-à-dire $d \in D(a) \cap D(b)$;*
- *Tout diviseur commun de a et b divise d c'est-à-dire $\forall n \in D(a) \cap D(b),\ n \mid d$.*

Exemple

- $(-12) \wedge 4 = 4$.
- $18 \wedge 27 = 9$.
- $8 \wedge 5 = 1$ *(dans ce cas on dit que 8 et 5 sont premiers entre eux).*

Définition

Soient a *et* b *deux entiers relatifs non tous les deux nuls. Un entier* $d \geq 1$ *est dit le plus grand commun diviseur de* a *et* b*, qu'on le note par* $\mathrm{pgcd}(a,b)$ *ou* $a \wedge b$*, si les deux conditions suivantes sont satisfaites :*

- d *est un diviseur commun de* a *et* b *c'est-à-dire* $d \in D(a) \cap D(b)$ *;*
- *Tout diviseur commun de* a *et* b *divise* d *c'est-à-dire* $\forall n \in D(a) \cap D(b),\ n \mid d$.

Exemple

- $(-12) \wedge 4 = 4$.
- $18 \wedge 27 = 9$.
- $8 \wedge 5 = 1$ *(dans ce cas on dit que* 8 *et* 5 *sont premiers entre eux).*
- *On peut utiliser le logiciel* $PARI$ *pour déterminer le plus grand commun diviseur de deux entiers* a *et* b *en utilisant la commande* $\mathrm{gcd}(a,b)$.

Propriétés

1. $a \wedge b = |a| \wedge |b|$.
2. $a \wedge b = b \wedge a$.
3. $a \wedge a = a \wedge 0 = |a|$ (avec $a \neq 0$).
4. $a \wedge (ka) = |a|$ $(\forall k \in \mathbb{Z})$.
5. $a \wedge 1 = 1$.
6. $(a \wedge b) \wedge c = a \wedge (b \wedge c)$.
7. $a \mid b \Longleftrightarrow a \wedge b = |a|$.
8. $k \mid a$ et $k \mid b \Longleftrightarrow k \mid a \wedge b$.
9. Soit $k \in \mathbb{Z}^*$, alors $(ka) \wedge (kb) = |k| \cdot a \wedge b$.
10. Soit $k \in \mathbb{Z}^*$ tel que $k \mid a$ et $k \mid b$, alors $\frac{a}{k} \wedge \frac{b}{k} = \frac{a \wedge b}{|k|}$.
11. $\frac{a}{a \wedge b} \wedge \frac{b}{a \wedge b} = 1$.

Preuve

1. Comme $D(a) \cap D(b) = D(|a|) \cap D(|b|)$, alors on aura le résultat.

Preuve

1. Comme $D(a) \cap D(b) = D(|a|) \cap D(|b|)$, alors on aura le résultat.
2. Trivial.

Preuve

1. Comme $D(a) \cap D(b) = D(|a|) \cap D(|b|)$, alors on aura le résultat.
2. Trivial.
3. Évident.

Preuve

1. Comme $D(a) \cap D(b) = D(|a|) \cap D(|b|)$, alors on aura le résultat.
2. Trivial.
3. Évident.
4. On a $D(a) \cap D(ka) = D(a)$ et $|a|$ est son plus grand élément, d'où le résultat.

Preuve

1. Comme $D(a)\cap D(b) = D(|a|)\cap D(|b|)$, alors on aura le résultat.
2. Trivial.
3. Évident.
4. On a $D(a)\cap D(ka) = D(a)$ et $|a|$ est son plus grand élément, d'où le résultat.
5. On a $D(a)\cap D(1) = D(1)$ et 1 est son plus grand élément, d'où le résultat.

Preuve

1. Comme $D(a) \cap D(b) = D(|a|) \cap D(|b|)$, alors on aura le résultat.
2. Trivial.
3. Évident.
4. On a $D(a) \cap D(ka) = D(a)$ et $|a|$ est son plus grand élément, d'où le résultat.
5. On a $D(a) \cap D(1) = D(1)$ et 1 est son plus grand élément, d'où le résultat.
6. On a $(D(a) \cap D(b)) \cap D(c) = D(a) \cap (D(b) \cap D(c))$, donc $(a \wedge b) \wedge c = a \wedge (b \wedge c)$.

Preuve

1. Comme $D(a) \cap D(b) = D(|a|) \cap D(|b|)$, alors on aura le résultat.
2. Trivial.
3. Évident.
4. On a $D(a) \cap D(ka) = D(a)$ et $|a|$ est son plus grand élément, d'où le résultat.
5. On a $D(a) \cap D(1) = D(1)$ et 1 est son plus grand élément, d'où le résultat.
6. On a $(D(a) \cap D(b)) \cap D(c) = D(a) \cap (D(b) \cap D(c))$, donc $(a \wedge b) \wedge c = a \wedge (b \wedge c)$.
7. Évident.

Preuve

1. Comme $D(a) \cap D(b) = D(|a|) \cap D(|b|)$, alors on aura le résultat.
2. Trivial.
3. Évident.
4. On a $D(a) \cap D(ka) = D(a)$ et $|a|$ est son plus grand élément, d'où le résultat.
5. On a $D(a) \cap D(1) = D(1)$ et 1 est son plus grand élément, d'où le résultat.
6. On a $(D(a) \cap D(b)) \cap D(c) = D(a) \cap (D(b) \cap D(c))$, donc $(a \wedge b) \wedge c = a \wedge (b \wedge c)$.
7. Évident.
8. Par définition du pgcd.

Preuve

1. Comme $D(a) \cap D(b) = D(|a|) \cap D(|b|)$, alors on aura le résultat.
2. Trivial.
3. Évident.
4. On a $D(a) \cap D(ka) = D(a)$ et $|a|$ est son plus grand élément, d'où le résultat.
5. On a $D(a) \cap D(1) = D(1)$ et 1 est son plus grand élément, d'où le résultat.
6. On a $(D(a) \cap D(b)) \cap D(c) = D(a) \cap (D(b) \cap D(c))$, donc $(a \wedge b) \wedge c = a \wedge (b \wedge c)$.
7. Évident.
8. Par définition du pgcd.
9. Soit $k \in \mathbb{Z}^*$, posons $d = (ka) \wedge (kb)$ et $\delta = a \wedge b$ et montrons que $d = |k|\delta$. On a $\delta = a \wedge b$, donc $\delta \mid a$ et $\delta \mid b$, donc $|k|\delta \mid ka$ et $|k|\delta \mid kb$, ainsi $|k|\delta \mid d$, donc $\exists n \in \mathbb{N}^*$ tel que $d = n|k|\delta$, ce qui donne $\exists n \in \mathbb{N}^*$ tel que $n|k|\delta \mid ka$ et $n|k|\delta \mid kb$, alors $\exists n \in \mathbb{N}^*$ tel que $n\delta \mid a$ et $n\delta \mid b$, donc $n\delta \mid \delta$, par suite $n = 1$, ce qui donne que $d = |k|\delta$.

Preuve

1. Comme $D(a)\cap D(b)=D(|a|)\cap D(|b|)$, alors on aura le résultat.
2. Trivial.
3. Évident.
4. On a $D(a)\cap D(ka)=D(a)$ et $|a|$ est son plus grand élément, d'où le résultat.
5. On a $D(a)\cap D(1)=D(1)$ et 1 est son plus grand élément, d'où le résultat.
6. On a $(D(a)\cap D(b))\cap D(c)=D(a)\cap(D(b)\cap D(c))$, donc $(a\wedge b)\wedge c=a\wedge(b\wedge c)$.
7. Évident.
8. Par définition du pgcd.
9. Soit $k\in\mathbb{Z}^*$, posons $d=(ka)\wedge(kb)$ et $\delta=a\wedge b$ et montrons que $d=|k|\delta$. On a $\delta=a\wedge b$, donc $\delta\mid a$ et $\delta\mid b$, donc $|k|\delta\mid ka$ et $|k|\delta\mid kb$, ainsi $|k|\delta\mid d$, donc $\exists n\in\mathbb{N}^*$ tel que $d=n|k|\delta$, ce qui donne $\exists n\in\mathbb{N}^*$ tel que $n|k|\delta\mid ka$ et $n|k|\delta\mid kb$, alors $\exists n\in\mathbb{N}^*$ tel que $n\delta\mid a$ et $n\delta\mid b$, donc $n\delta\mid\delta$, par suite $n=1$, ce qui donne que $d=|k|\delta$.
10. Soit $k\in\mathbb{Z}^*$ tel que $k\mid a$ et $k\mid b$.
    On a
$$\mathrm{pgcd}(a,\ b)=\mathrm{pgcd}(k\cdot\frac{a}{k},\ k\cdot\frac{b}{k})=|k|\cdot\mathrm{pgcd}(\frac{a}{k},\ \frac{b}{k})\Rightarrow\mathrm{pgcd}(\frac{a}{k},\ \frac{b}{k})=\frac{\mathrm{pgcd}(a,\ b)}{|k|}.$$

Preuve

1. Comme $D(a) \cap D(b) = D(|a|) \cap D(|b|)$, alors on aura le résultat.
2. Trivial.
3. Évident.
4. On a $D(a) \cap D(ka) = D(a)$ et $|a|$ est son plus grand élément, d'où le résultat.
5. On a $D(a) \cap D(1) = D(1)$ et 1 est son plus grand élément, d'où le résultat.
6. On a $(D(a) \cap D(b)) \cap D(c) = D(a) \cap (D(b) \cap D(c))$, donc $(a \wedge b) \wedge c = a \wedge (b \wedge c)$.
7. Évident.
8. Par définition du pgcd.
9. Soit $k \in \mathbb{Z}^*$, posons $d = (ka) \wedge (kb)$ et $\delta = a \wedge b$ et montrons que $d = |k|\delta$.
   On a $\delta = a \wedge b$, donc $\delta \mid a$ et $\delta \mid b$, donc $|k|\delta \mid ka$ et $|k|\delta \mid kb$, ainsi $|k|\delta \mid d$, donc $\exists n \in \mathbb{N}^*$ tel que $d = n|k|\delta$, ce qui donne $\exists n \in \mathbb{N}^*$ tel que $n|k|\delta \mid ka$ et $n|k|\delta \mid kb$, alors $\exists n \in \mathbb{N}^*$ tel que $n\delta \mid a$ et $n\delta \mid b$, donc $n\delta \mid \delta$, par suite $n = 1$, ce qui donne que $d = |k|\delta$.
10. Soit $k \in \mathbb{Z}^*$ tel que $k \mid a$ et $k \mid b$.
    On a
    $$\mathrm{pgcd}(a,\ b) = \mathrm{pgcd}(k \cdot \frac{a}{k},\ k \cdot \frac{b}{k}) = |k| \cdot \mathrm{pgcd}(\frac{a}{k},\ \frac{b}{k}) \Rightarrow \mathrm{pgcd}(\frac{a}{k},\ \frac{b}{k}) = \frac{\mathrm{pgcd}(a,\ b)}{|k|}.$$
11. En utilisant 10, on trouve $\frac{a}{a \wedge b} \wedge \frac{b}{a \wedge b} = \frac{a \wedge b}{a \wedge b} = 1$.

Proposition

Soient a et b deux entiers relatifs avec $b \neq 0$. Si r est le reste de la division euclidienne de a par b, alors $a \wedge b = b \wedge r$.

Proposition

Soient a et b deux entiers relatifs avec $b \neq 0$. Si r est le reste de la division euclidienne de a par b, alors $a \wedge b = b \wedge r$.

Preuve.

Il suffit de remarquer que si r est le reste de la division euclidienne de a par b, alors les diviseurs communs de a et b sont ceux de b et r.

$$D(a) \cap D(b) = D(b) \cap D(r).$$



L'algorithme d'Euclide est basé sur la proposition précédente et permet le calcul du pgcd de deux entiers en effectuant un nombre fini de divisions euclidiennes.
Soient a et b deux entiers strictement positifs, on pose $r_0 = a$ et $r_1 = b$, et tant que $r_i > 0$ en effectue les divisions euclidiennes suivantes :

$$r_0 = r_1 q_1 + r_2 \text{ où } 0 \leq r_2 < r_1;$$
$$r_1 = r_2 q_2 + r_3 \text{ où } 0 \leq r_3 < r_2;$$
$$\vdots$$
$$r_{k-2} = r_{k-1} q_{k-1} + r_k \text{ où } 0 \leq r_k < r_{k-1};$$
$$r_{k-1} = r_k q_k + r_{k+1} \text{ où } 0 \leq r_{k+1} < r_k$$

La suite $r_1, r_2, r_3, \dots$ est une suite décroissante d'entiers positifs, on obtient nécessairement un reste nul au bout d'un nombre fini de divisions.
Il résulte de la proposition précédente que pour chaque $k \geq 0$, on a $a \wedge b = r_k \wedge r_{k+1}$.
Notons par r_n le dernier reste non nul, on a donc $r_{n+1} = 0$, donc

$$a \wedge b = r_n \wedge r_{n+1} = r_n \wedge 0 = r_n.$$

Remarque

1. *On effectue les divisions euclidiennes successives décrites précédement jusqu'à ce qu'on obtient un reste nul, le* $\operatorname{pgcd}(a,b)$ *est le dernier reste non nul.*
2. *Il existe* u *et* v *dans* $\mathbb{Z}$ *tel que* $\operatorname{pgcd}(a,b) = au + bv$.
   Pour determiner u *et* v*, il suffit de considérer l'algorithme d'Euclide inversement en remplaçant le reste dans l'étape* i *par son expression dans l'étape* $i-1$.
   Les entiers u *et* v *sont appelés les coefficients de Bézout.*

Exemple

Soient $a = 600$ *et* $b = 124$.

Exemple

Soient $a = 600$ *et* $b = 124$.
On a

$$\begin{aligned} 600 &= 124\times 4+104; \\ 124 &= 104\times 1+20; \\ 104 &= 20\times 5+4; \\ 20 &= 4\times 5+0. \end{aligned} \quad \textit{et} \quad \begin{aligned} 4 &= 104-20\times 5; \\ 4 &= 104-(124-104\times 1)\times 5; \\ 4 &= (600-124\times 4)\times 6+124\times(-5); \\ 4 &= 600\times 6+124\times(-24)+124\times(-5); \\ 4 &= 600\times 6+124\times(-29). \end{aligned}$$

Ainsi $\mathrm{pgcd}(600,124) = 4 = 600\times 6+124\times(-29)$ *(*$u = 6$ *et* $v = -29$*).*

Exemple

Soient $a = -326$ *et* $b = 15$.

Exemple

Soient $a = -326$ *et* $b = 15$.
On a

$$\begin{array}{rlcrl} -326 & = 15 \times (-22) + 4; & et & 1 & = 4 - 3 \times 1; \\ 15 & = 4 \times 3 + 3; & & & = 4 - (15 - 4 \times 3); \\ 4 & = 3 \times 1 + 1; & & & = 4 - 15 + 4 \times 3; \\ 3 & = 1 \times 3 + 0. & & & = 4 \times 4 - 15; \\ & & & & = 4 \times (-326 - 15 \times (-22)) - 15; \\ & & & & = (-326) \times 4 + 15 \times 88 - 15; \\ & & & & = (-326) \times 4 + 15 \times 87. \end{array}$$

Ainsi $\text{pgcd}(-326, 15) = 1 = (-326) \times 4 + 15 \times 87$ *(*$u = 4$ *et* $v = 87$*).*

Définition (Nombres premiers entre eux)

Soient a et b deux entiers relatifs, on dit que a et b sont premiers entre eux si $a \wedge b = 1$.

Définition (Nombres premiers entre eux)

Soient a *et* b *deux entiers relatifs, on dit que* a *et* b *sont premiers entre eux si* $a \wedge b = 1$.

Théorème (Théorème de Bézout)

Soient a *et* b *deux entiers relatifs, alors* a *et* b *sont premiers entre eux si et seulement si il existe deux entiers* u *et* v *tel que* $au + bv = 1$.

Définition (Nombres premiers entre eux)

Soient a et b deux entiers relatifs, on dit que a et b sont premiers entre eux si $a \wedge b = 1$.

Théorème (Théorème de Bézout)

Soient a et b deux entiers relatifs, alors a et b sont premiers entre eux si et seulement si il existe deux entiers u et v tel que $au + bv = 1$.

Preuve.

Si a et b sont premiers entre eux, alors $a \wedge b = 1$ et d'après l'algorithme d'Euclide il existe des entiers u et v tel que $au + bv = 1$.
Inversement s'il existe des entiers u et v tel que $au + bv = 1$. Posons $d = a \wedge b$, donc $d \mid au + bv$, ainsi $d \mid 1$, ce qui donne que a et b sont premiers entre eux. □

Corollaire (Lemme de Gauss)

Soient a, b et c trois entiers relatifs. Si a divise le produit bc et a est premier avec b, alors a divise c.

Corollaire (Lemme de Gauss)

Soient a, b et c trois entiers relatifs. Si a divise le produit bc et a est premier avec b, alors a divise c.

Preuve.

Comme $a \mid bc$, alors $(\exists k \in \mathbb{Z}) : bc = ka$. Puisque $a \wedge b = 1$, alors d'après le théorème de Bézout, $(\exists (u,v) \in \mathbb{Z}^2) : au + bv = 1$, donc

$$c = auc + bvc = auc + kav = a(cu + kv),$$

ce qui donne que $a \mid c$. 

Proposition

Soient a, b et c trois entiers relatifs, alors :

1. *Si $(a,b) \neq (0,0)$ on a :*

$$a \wedge b = d \Longleftrightarrow \exists (a',b') \in \mathbb{Z}^2 : a' \wedge b' = 1,\ a = a'd \text{ et } b = b'd.$$

2. *Si $a \mid c$, $b \mid c$ et $a \wedge b = 1$, alors $ab \mid c$.*
3. *Si $a \wedge b = 1$ et $a \wedge c = 1$, alors $a \wedge bc = 1$.*
4. *Si $a \wedge b = 1$, alors $\forall (m,n) \in \mathbb{N}^2$ on a : $a^m \wedge b^n = 1$.*

Preuve.

1. Si $a \wedge b = d$, alors $\exists (a', b') \in \mathbb{Z}^2 : a = a'd$ et $b = b'd$, ainsi $d = a \wedge b = a'd \wedge b'd = d(a' \wedge b')$, ce qui donne $\exists (a', b') \in \mathbb{Z}^2 : a' \wedge b' = 1$, $a = a'd$ et $b = b'd$.
   Inversement, si $\exists (a', b') \in \mathbb{Z}^2 : a' \wedge b' = 1$, $a = a'd$ et $b = b'd$, alors $a \wedge b = a'd \wedge b'd = d(a' \wedge b') = d$.

Preuve.

1. Si $a \wedge b = d$, alors $\exists(a',b') \in \mathbb{Z}^2 : a = a'd$ et $b = b'd$, ainsi $d = a \wedge b = a'd \wedge b'd = d(a' \wedge b')$, ce qui donne $\exists(a',b') \in \mathbb{Z}^2 : a' \wedge b' = 1$, $a = a'd$ et $b = b'd$.
   Inversement, si $\exists(a',b') \in \mathbb{Z}^2 : a' \wedge b' = 1$, $a = a'd$ et $b = b'd$, alors $a \wedge b = a'd \wedge b'd = d(a' \wedge b') = d$.
2. On a $a \mid c$, donc $\exists k \in \mathbb{Z}$ tel que $c = ka$, ainsi $b \mid ka$ et on a $a \wedge b = 1$, donc d'après le lemme de Gauss on trouve que $b \mid k$, il existe donc $k' \in \mathbb{Z}$ tel que $k = k'b$, alors il existe $k' \in \mathbb{Z}$ tel que $c = k'ab$, ce qui donne que $ab \mid c$.

Preuve.

1. Si $a \wedge b = d$, alors $\exists (a', b') \in \mathbb{Z}^2 : a = a'd$ et $b = b'd$, ainsi $d = a \wedge b = a'd \wedge b'd = d(a' \wedge b')$, ce qui donne $\exists (a', b') \in \mathbb{Z}^2 : a' \wedge b' = 1$, $a = a'd$ et $b = b'd$.
   Inversement, si $\exists (a', b') \in \mathbb{Z}^2 : a' \wedge b' = 1$, $a = a'd$ et $b = b'd$, alors $a \wedge b = a'd \wedge b'd = d(a' \wedge b') = d$.
2. On a $a \mid c$, donc $\exists k \in \mathbb{Z}$ tel que $c = ka$, ainsi $b \mid ka$ et on a $a \wedge b = 1$, donc d'après le lemme de Gauss on trouve que $b \mid k$, il existe donc $k' \in \mathbb{Z}$ tel que $k = k'b$, alors il existe $k' \in \mathbb{Z}$ tel que $c = k'ab$, ce qui donne que $ab \mid c$.
3. On a $a \wedge b = 1$, alors il existe $(u, v) \in \mathbb{Z}^2 : au + bv = 1$ et on a $a \wedge c = 1$, donc il existe $(u', v') \in \mathbb{Z}^2 : au' + cv' = 1$, ainsi

   $$1 = (au + bv)(au' + cv') = a \cdot (auu' + cuv' + nvu') + bc \cdot (vv'),$$

   ce qui donne, d'après le théorème de Bézout, que $a \wedge bc = 1$.
4. Conséquence de 3.



Définition

Soient a et b deux entiers relatifs tous deux non nuls. Un entier $m \geq 1$ est dit le plus petit commun multiple de a et b, qu'on le note par $\mathrm{ppcm}(a,b)$ ou $a \vee b$, si les deux conditions suivantes sont satisfaites :

- *m est un multiple commun de a et b ;*
- *Tout multiple commun de a et b est multiple de m.*

Définition

Soient a *et* b *deux entiers relatifs tous deux non nuls. Un entier* $m \geq 1$ *est dit le plus petit commun multiple de* a *et* b*, qu'on le note par* $\mathrm{ppcm}(a,b)$ *ou* $a \vee b$*, si les deux conditions suivantes sont satisfaites :*

- m *est un multiple commun de* a *et* b *;*
- *Tout multiple commun de* a *et* b *est multiple de* m*.*

Exemple

- $(-12) \vee 4 =$

Définition

Soient a et b deux entiers relatifs tous deux non nuls. Un entier $m \geq 1$ est dit le plus petit commun multiple de a et b, qu'on le note par $\mathrm{ppcm}(a,b)$ ou $a \vee b$, si les deux conditions suivantes sont satisfaites :

- *m est un multiple commun de a et b ;*
- *Tout multiple commun de a et b est multiple de m.*

Exemple

- $(-12) \vee 4 = 12.$
- $4 \vee 6 =$

Définition

Soient a et b deux entiers relatifs tous deux non nuls. Un entier $m \geq 1$ est dit le plus petit commun multiple de a et b, qu'on le note par $\mathrm{ppcm}(a,b)$ ou $a \vee b$, si les deux conditions suivantes sont satisfaites :

- *m est un multiple commun de a et b ;*
- *Tout multiple commun de a et b est multiple de m.*

Exemple

- $(-12) \vee 4 = 12.$
- $4 \vee 6 = 12.$
- $8 \vee 5 =$

Définition

Soient a et b deux entiers relatifs tous deux non nuls. Un entier $m \geq 1$ est dit le plus petit commun multiple de a et b, qu'on le note par $\mathrm{ppcm}(a,b)$ ou $a \vee b$, si les deux conditions suivantes sont satisfaites :

- *m est un multiple commun de a et b ;*
- *Tout multiple commun de a et b est multiple de m.*

Exemple

- $(-12) \vee 4 = 12.$
- $4 \vee 6 = 12.$
- $8 \vee 5 = 40.$

Définition

Soient a *et* b *deux entiers relatifs tous deux non nuls. Un entier* $m \geq 1$ *est dit le plus petit commun multiple de* a *et* b*, qu'on le note par* $\operatorname{ppcm}(a,b)$ *ou* $a \vee b$*, si les deux conditions suivantes sont satisfaites :*

- m *est un multiple commun de* a *et* b *;*
- *Tout multiple commun de* a *et* b *est multiple de* m*.*

Exemple

- $(-12) \vee 4 = 12$.
- $4 \vee 6 = 12$.
- $8 \vee 5 = 40$.
- *On peut utiliser le logiciel PARI pour déterminer le plus petit commun multiple de deux entiers* a *et* b *en utilisant la commande* $\operatorname{lcm}(a,b)$*.*

Propriétés

1. $a \vee b = b \vee a.$
2. $a \vee b = |a| \vee |b|.$
3. $a \vee a = |a|.$
4. $b \mid a \Longleftrightarrow a \vee b = |a|.$
5. $a \vee 1 = |a|.$
6. $a \vee 0 = 0.$
7. $a \vee b \mid ab.$
8. $(a \vee b) \vee c = a \vee (b \vee c).$
9. $(ka) \vee (kb) = |k| \cdot a \vee b,\ \forall k \in \mathbb{Z}.$

Preuve.

Les propriétés 1, 2, 3, 4, 5 et 6 sont triviales.

7. On a $a \mid ab$ et $b \mid ab$, donc $a \vee b \mid ab$, par définition du ppcm.
8. Si $abc = 0$, alors $(a \vee b) \vee c = a \vee (b \vee c) = 0$. Si $abc \neq 0$, on remarque que $(a \vee b) \vee c$ est le plus petit élément de l'ensemble $[(a\mathbb{Z} \cap b\mathbb{Z}) \cap c\mathbb{Z}] \cap \mathbb{N}^*$ et $a \vee (b \vee c)$ est le plus petit élément de l'ensemble $[a\mathbb{Z} \cap (b\mathbb{Z} \cap c\mathbb{Z})] \cap \mathbb{Z}^*$, or les deux ensembles sont égaux, donc $(a \vee b) \vee c = a \vee (b \vee c)$.



Proposition

Soient a et b deux entiers relatifs tel que $ab \neq 0$, $d = a \wedge b$ et $m = a \vee b$. Si on pose $a = da'$ et $b = db'$, alors $a' \wedge b' = 1$ et $m = d \cdot |a'b'|$.
En particulier on a :

$$dm = (a \wedge b) \times (a \vee b) = |ab|.$$

Preuve.

Posons $m' = d \cdot |a'b'|$. Il est clair que m' est un multiple commun de a et de b. Montrons que c'est le ppcm de a et b en montrant qu'il divise tout multiple commun de a et b.

Soit m'' un multiple commun de a et de b. C'est un multiple de a, donc il existe un entier p tel que $m'' = ap = da'p$. C'est un multiple de b donc il existe un entier q tel que $m'' = bq = db'q$. Par conséquent $da'p = db'q$ et donc $a'p = b'q$. En appliquant le théorème de Gauss, sachant que a' divise $b'q$ et est premier avec b', on peut déduire que a' divise q et qu'il existe un entier r tel que $q = ra'$.

On a obtenu $m'' = db'ra' = (da'b')r$ et donc m'' est un multiple de m' ce qui démontre que m' est le ppcm de a et de b. En particulier on a

$$(a \wedge b) \times (a \vee b) = d^2|a'b'| = (d|a'|) \cdot (d|b'|) = |ab|.$$



Preuve.

Posons $m' = d \cdot |a'b'|$. Il est clair que m' est un multiple commun de a et de b. Montrons que c'est le ppcm de a et b en montrant qu'il divise tout multiple commun de a et b.
Soit m'' un multiple commun de a et de b. C'est un multiple de a, donc il existe un entier p tel que $m'' = ap = da'p$. C'est un multiple de b donc il existe un entier q tel que $m'' = bq = db'q$. Par conséquent $da'p = db'q$ et donc $a'p = b'q$. En appliquant le théorème de Gauss, sachant que a' divise $b'q$ et est premier avec b', on peut déduire que a' divise q et qu'il existe un entier r tel que $q = ra'$.
On a obtenu $m'' = db'ra' = (da'b')r$ et donc m'' est un multiple de m' ce qui démontre que m' est le ppcm de a et de b. En particulier on a

$$(a \wedge b) \times (a \vee b) = d^2|a'b'| = (d|a'|) \cdot (d|b'|) = |ab|.$$

□

Remarque

Soient a et b deux entiers relatifs, alors

$$a \vee b = |ab| \Longleftrightarrow a \wedge b = 1.$$

Proposition

Soit p *un nombre premier. Si* p *divise le produit* $n_1 n_2 \ldots n_k$ *de* k *entiers, alors il existe au mions* $i_0 \in \{1, 2, \ldots, k\}$ *tel que* p *divise* n_{i_0}.

Proposition

Soit p un nombre premier. Si p divise le produit $n_1 n_2 \ldots n_k$ de k entiers, alors il existe au mions $i_0 \in \{1,2,\ldots,k\}$ tel que p divise n_{i_0}.

Preuve.

Supposons que p ne divise aucun des n_i pour tout $i \in \{1,2,\ldots,k\}$, alors $p \wedge n_i = 1$ pour tout $i \in \{1,2,\ldots,k\}$, or on sait que si $a \wedge b = 1$ et $a \wedge c = 1$, alors $a \wedge bc = 1$, donc $p \wedge n_1 n_2 \ldots n_k = 1$, ce qui est absurde, ainsi il existe au mions $i_0 \in \{1,2,\ldots,k\}$ tel que p divise n_{i_0}. □

Théorème (Théorème fondamental de l'arithmétique)

Tout entier $n > 1$ *s'écrit de façon unique sous la forme* $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, *où les* p_i *sont des entiers premiers vérifiant* $p_1 < p_2 < \dots < p_k$ *et les* α_i *sont des entiers strictement positifs.*

Preuve.

- **Existence** : Soit p_1 le plus petit diviseur premier de n. L'ensemble des entiers $\alpha > 0$ tel que p_1^{α} divise n est fini, soit donc α_1 le plus grand des α, alors α_1 est l'unique entier ≥ 1 tel que $p_1^{\alpha_1} \mid n$ et $p_1^{\alpha_1+1} \nmid n$.
On a donc $n = p_1^{\alpha_1} k_1$ avec $k_1 \in \mathbb{N}^*$, ainsi si $k_1 = 1$, alors c'est terminé, sinon on reprend le même procédé avec k_1. On recomence donc l'opération jusqu'à obtenir un quotient $k_i = 1$, ce qui arrive au bout d'un nombre fini d'opération car $n > k_1 > \ldots \geq 1$.
- **Unicité** : Supposons que

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \ldots q_r^{\beta_r} \quad (*)$$

où les $p_i,\ q_j,\ \alpha_i,\ \beta_j$ vérifient les conditions du théorème et montrons que $k = r$, $p_i = q_i$ et $\alpha_i = \beta_i\ \forall i \in \{1, 2, \ldots, k\}$. Supposons que $r > k$, alors il existe $j \in \{1, \ldots, r\}$ tel que $q_j \neq p_i\ \forall i \in \{1, \ldots, k\}$, ainsi $q_j \wedge n = 1$, ce qui est absurde, ainsi $k = r$ et $(p_1, p_2, \ldots, p_k) = (q_1, q_2, \ldots, q_k)$. Enfin, supposons qu'il existe i tel que $\alpha_i \neq \beta_i$ et posons $s = \inf(\alpha_i, \beta_i)$, alors par division des deux membres de la relation $(*)$ par p_i^s, on trouve que p_i divise un produit de nombres premiers tous différents de lui même, ce qui est impossible, d'où le résultat. □

Remarque

- *Tout entier relatif non nul* n *s'écrit sous la forme* $n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, *où les* p_i *sont des entiers premiers vérifiant* $p_1 < p_2 < \dots < p_k$ *et les* α_i *sont des entiers naturels.*
- *Pour deux entiers relatifs non nuls* a *et* b, *on peut toujours prendre les mêmes nombres premiers dans les décompositions de* a *et de* b *en facteurs premiers en posant des puissances nuls pour les premiers qui ne figurent pas dans l'une des deux décompositions.*

Corollaire

Soient a et b deux entiers relatifs non nuls et $a = up_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$, $b = vp_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$ avec $u = \pm 1$, $v = \pm 1$, $\alpha_i, \beta_i \in \mathbb{N}$ et les p_i des nombres premiers vérifiant $p_1 < p_2 < \dots < p_n$, alors :

$$\mathrm{pgcd}(a,b) = \prod_i^n p_i^{\inf(\alpha_i,\beta_i)} \quad \textbf{et} \quad \mathrm{ppcm}(a,b) = \prod_i^n p_i^{\sup(\alpha_i,\beta_i)}$$

Corollaire

Soient a et b deux entiers relatifs non nuls et $a = up_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$, $b = vp_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$ avec $u = \pm 1$, $v = \pm 1$, $\alpha_i, \beta_i \in \mathbb{N}$ et les p_i des nombres premiers vérifiant $p_1 < p_2 < \dots < p_n$, alors :

$$\mathrm{pgcd}(a,b) = \prod_i^n p_i^{\inf(\alpha_i,\beta_i)} \quad \textbf{et} \quad \mathrm{ppcm}(a,b) = \prod_i^n p_i^{\sup(\alpha_i,\beta_i)}$$

Preuve.

La preuve de ce théorème se découle facilement du théorème fondamental de l'arithmétique.



Exemple

- *Pour* $68 =$

Exemple

- *Pour* $68 = 2^2 \times 3^0 \times 7^0 \times 17^1$ *et* $84 =$

Exemple

- *Pour* $68 = 2^2 \times 3^0 \times 7^0 \times 17^1$ *et* $84 = 2^2 \times 3^1 \times 7^1 \times 17^0$, *on a :*

  $68 \wedge 84 =$

Exemple

- *Pour* $68 = 2^2 \times 3^0 \times 7^0 \times 17^1$ *et* $84 = 2^2 \times 3^1 \times 7^1 \times 17^0$, *on a :*

  $68 \wedge 84 = 2^2 \times 3^0 \times 7^0 \times 17^0 = 4$ *et* $68 \vee 84 =$

Exemple

- *Pour* $68 = 2^2 \times 3^0 \times 7^0 \times 17^1$ *et* $84 = 2^2 \times 3^1 \times 7^1 \times 17^0$, *on a :*

$$68 \wedge 84 = 2^2 \times 3^0 \times 7^0 \times 17^0 = 4 \text{ et } 68 \vee 84 = 2^2 \times 3^1 \times 7^1 \times 17^1 = 1428.$$

Exemple

- *Pour* $68 = 2^2 \times 3^0 \times 7^0 \times 17^1$ *et* $84 = 2^2 \times 3^1 \times 7^1 \times 17^0$, *on a :*

$$68 \wedge 84 = 2^2 \times 3^0 \times 7^0 \times 17^0 = 4 \text{ et } 68 \vee 84 = 2^2 \times 3^1 \times 7^1 \times 17^1 = 1428.$$

- *On peut utiliser le logiciel* $PARI$ *pour factoriser un entier* a *en utilisant la commande "*$\mathrm{factor}(a)$*".*

Théorème (Nombre de diviseurs)

Soient a *un entier naturel strictement supérieur à* 1 *et* $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ *sa décomposition en produit de facteurs premiers, alors le nombre de diviseurs positifs de* a *est* $N = (1+\alpha_1)(1+\alpha_2)\dots(1+\alpha_k)$.

Théorème (Nombre de diviseurs)

Soient a un entier naturel strictement supérieur à 1 et $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ sa décomposition en produit de facteurs premiers, alors le nombre de diviseurs positifs de a est $N = (1+\alpha_1)(1+\alpha_2)\dots(1+\alpha_k)$.

Preuve.

Soit d un diviseur positif de a, alors $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ avec $0 \leq \beta_i \leq \alpha_i$ $(\forall i \in \{1, \dots, k\})$, donc il y a $(1+\alpha_i)$ valeurs possibles de β_i et d'après le principe fondamentale du dénombrement il y aura N diviseurs de a □

Théorème (Nombre de diviseurs)

Soient a *un entier naturel strictement supérieur à* 1 *et* $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ *sa décomposition en produit de facteurs premiers, alors le nombre de diviseurs positifs de* a *est* $N = (1+\alpha_1)(1+\alpha_2)\dots(1+\alpha_k)$.

Preuve.

Soit d un diviseur positif de a, alors $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ avec $0 \leq \beta_i \leq \alpha_i$ $(\forall i \in \{1, \dots, k\})$, donc il y a $(1+\alpha_i)$ valeurs possibles de β_i et d'après le principe fondamentale du dénombrement il y aura N diviseurs de a □

Exemple

Le nombre de diviseurs positifs de $504 =$

Théorème (Nombre de diviseurs)

Soient a *un entier naturel strictement supérieur à* 1 *et* $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ *sa décomposition en produit de facteurs premiers, alors le nombre de diviseurs positifs de* a *est* $N = (1+\alpha_1)(1+\alpha_2)\dots(1+\alpha_k)$*.*

Preuve.

Soit d un diviseur positif de a, alors $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ avec $0 \leq \beta_i \leq \alpha_i$ $(\forall i \in \{1, \dots, k\})$, donc il y a $(1+\alpha_i)$ valeurs possibles de β_i et d'après le principe fondamentale du dénombrement il y aura N diviseurs de a □

Exemple

Le nombre de diviseurs positifs de $504 = 2^3 \times 3^2 \times 7$ *est*

$$(1+3) \times (1+2) \times (1+1) = 24.$$

Pour trouver le nombre de diviseurs de 504 *dans* $\mathbb{Z}$ *on multiplie le Le nombre de diviseurs positifs par* 2*, aini le nombre de diviseurs de* 504 *dans* $\mathbb{Z}$ *est* $2 \times 24 = 48$*.*

Définition

Soient E *un ensemble non vide et* $\mathcal{R}$ *une relation sur* E*. On dit que* $\mathcal{R}$ *est une relation d'équivalence sur* E *si elle est :*

- *réflexive :* $\forall x \in E,\ x\mathcal{R}x$ *;*
- *symétrique :* $\forall x \in E,\ \forall y \in E,\ x\mathcal{R}y \Longrightarrow y\mathcal{R}x$ *;*
- *transitive :* $\forall x \in E,\ \forall y \in E,\ \forall z \in E,\ (x\mathcal{R}y \text{ et } y\mathcal{R}z) \Longrightarrow x\mathcal{R}z$ *;*

Dans le cas d'une relation d'équivalence, deux éléments en relation sont aussi dits équivalents.

Définition (Classe d'équivalence)

Soit E *un ensemble muni d'une relation d'équivalence* $\mathcal{R}$*. On appelle classe d'équivalence d'un élément* $x \in E$ *l'ensemble :* $\mathfrak{cl}(x) = \{y \in E \mid x \mathcal{R} y\}$.

Définition (Classe d'équivalence)

Soit E *un ensemble muni d'une relation d'équivalence* $\mathcal{R}$*. On appelle classe d'équivalence d'un élément* $x \in E$ *l'ensemble :* $\mathfrak{cl}(x) = \{y \in E \mid x\mathcal{R}y\}$.

Remarque

Toute classe d'équivalence contient au moins un élément.

Théorème

Soit E un ensemble muni d'une relation d'équivalence $\mathcal{R}$ et soient $\mathfrak{cl}(x)$ et $\mathfrak{cl}(y)$ les classes de deux éléments x et y de E, alors ces classes sont disjointes ou sont confondues.

Théorème

Soit E un ensemble muni d'une relation d'équivalence $\mathcal{R}$ et soient $\mathfrak{cl}(x)$ et $\mathfrak{cl}(y)$ les classes de deux éléments x et y de E, alors ces classes sont disjointes ou sont confondues.

Preuve.

Si x et y sont équivalents, alors $x\mathcal{R}y$. Soit $z \in C_{\mathfrak{cl}}(x)$, donc $x\mathcal{R}z$, ainsi $y\mathcal{R}z$, d'où $z \in \mathfrak{cl}(y)$, ce qui donne que $\mathfrak{cl}(x) \subseteq \mathfrak{cl}(y)$ et puis que dans ce cas x et y jouent des rôles symétriques on trouve que $\mathfrak{cl}(x) = \mathfrak{cl}(y)$.
Si x et y ne sont pas équivalents. Soit $z \in \mathfrak{cl}(x)$, donc $x\mathcal{R}z$, ainsi si $z \in \mathfrak{cl}(y)$, alors $y\mathcal{R}z$ d'où $x\mathcal{R}y$ ce qui n'est pas le cas, d'où $z \notin \mathfrak{cl}(y)$ et puis que dans ce cas x et y jouent des rôles symétriques on trouve que $\mathfrak{cl}(x) \cap \mathfrak{cl}(y) = \emptyset$. □

Définition (Représentant d'une classe)

$\mathfrak{cl}(x)$ est la classe d'équivalence de tout élément a de $\mathfrak{cl}(x)$.
En effet, si a et b appartiennent à la classe de x, alors leurs classes sont confondues avec celle de x. Ceci justifie d'appeler tout élément d'une classe un représentant de cette classe.

Définition (Représentant d'une classe)

$\mathfrak{cl}(x)$ *est la classe d'équivalence de tout élément* a *de* $\mathfrak{cl}(x)$.
En effet, si a *et* b *appartiennent à la classe de* x*, alors leurs classes sont confondues avec celle de* x*. Ceci justifie d'appeler tout élément d'une classe un représentant de cette classe.*

Remarque

Soient E *un ensemble et* $\mathcal{R}$ *une relation d'équivalence sur* E*, alors :*

- *Chaque élément de* E *appartient à une classe au moins ;*
- *Chaque élément de* E *appartient à une seule classe.*

Ainsi l'ensemble de toutes les classes disjointes forment une partition de l'ensemble E.

Exemple

- *Sur tout ensemble E, l'égalité de deux éléments est une relation d'équivalence sur E.*
  Pour tout $x \in E$, on a $\mathfrak{cl}(x) = \{x\}$.
- *Sur l'ensemble des droites (du plan ou de l'espace), la relation "droites parallèles ou confondues" est une relation d'équivalence.*
  Pour toute droite d, on a $\mathfrak{cl}(d)$ est par définition la direction de d.
- *Pour les angles du plan, la relation de congruence modulo 2π est une relation d'équivalence.*
  La classe d'équivalence d'un angle par la relation de congruence modulo 2π est l'angle lui-même modulo 2π.
- *Dans $\mathbb{N} \times \mathbb{N}$ la relation $\mathcal{R}$ définie par $(a,b)\mathcal{R}(a',b') \Longleftrightarrow a+b' = a'+b$ est une relation d'équivalence.*
  La classe de (a,b) est par définition le nombre relatif $a-b$.
- *Dans $\mathbb{Z} \times \mathbb{Z}^*$ la relation $\mathcal{R}$ définie par $(a,b)\mathcal{R}(a',b') \Longleftrightarrow ab' = a'b$ est une relation d'équivalence.*
  La classe de (a,b) est par définition le nombre rationnel $\frac{a}{b}$.

Définition (Ensemble quotient)

L'ensemble des classes d'équivalence se nomme ensemble quotient de E par $\mathcal{R}$ et se note $E/\mathcal{R}$.
L'application $E \longrightarrow E/\mathcal{R}$ qui à tout élément x de E associe sa classe d'équivalence se nomme application (ou projection) canonique.

Définition

Soit n un entier strictement positif. On dit que deux entiers relatifs a et b sont congrus modulo n et on note $a \equiv b \pmod{n}$ ou $a \equiv b[n]$ si $(b-a)$ est un multiple de n (ou n divise $(b-a)$). On écrit

$$a \equiv b \pmod{n} \iff b-a \in n\mathbb{Z} \iff n \mid b-a.$$

Définition

Soit n un entier strictement positif. On dit que deux entiers relatifs a et b sont congrus modulo n et on note $a \equiv b \pmod{n}$ ou $a \equiv b[n]$ si $(b-a)$ est un multiple de n (ou n divise $(b-a)$). On écrit

$$a \equiv b \pmod{n} \Longleftrightarrow b-a \in n\mathbb{Z} \Longleftrightarrow n \mid b-a.$$

Exemple

- $31 \equiv 3 \pmod{14}$ *car* $14 \mid 31-3=28$.
- $53 \equiv -3 \pmod{7}$ *car* $7 \mid 53-(-3)=56$.

Proposition

Soient $n \in \mathbb{N}^*$, $a,\ b,\ c \in \mathbb{Z}$, *alors :*

1. $a \equiv a \pmod{n}$.
2. $a \equiv b \pmod{n} \Leftrightarrow b \equiv a \pmod{n}$.
3. *Si* $a \equiv b \pmod{n}$ *et* $b \equiv c \pmod{n}$, *alors* $a \equiv c \pmod{n}$.

Ainsi la relation de congruence modulo n *est une relation d'équivalence sur* $\mathbb{Z}$.

Proposition

Soient $n \in \mathbb{N}^*$, $a,\ b,\ c \in \mathbb{Z}$, alors :

1. $a \equiv a \pmod{n}$.
2. $a \equiv b \pmod{n} \Leftrightarrow b \equiv a \pmod{n}$.
3. *Si* $a \equiv b \pmod{n}$ *et* $b \equiv c \pmod{n}$, *alors* $a \equiv c \pmod{n}$.

Ainsi la relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.

Preuve.

1. On a $\mid (a-a) = 0$, donc $a \equiv a \pmod{n}$.
2. On a : $a \equiv b \pmod{n} \Leftrightarrow n \mid (b-a) \Leftrightarrow n \mid (a-b) \Leftrightarrow b \equiv a \pmod{n}$.
3. Si $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$, alors $n \mid (b-a)$ et $n \mid (c-b)$, donc $n \mid (c-b)+(b-a) = (c-a)$, ainsi $a \equiv c \pmod{n}$.



Propriétés

Soient $n \in \mathbb{N}^*$, $a,\ b,\ c,\ d \in \mathbb{Z}$, *alors :*

1. $a \equiv b \pmod{n} \Leftrightarrow a$ *et* b *ont le même reste dans la division euclidienne par* n.
2. *Si* $a \equiv c \pmod{n}$ *et* $b \equiv d \pmod{n}$, *alors* $a + b \equiv c + d \pmod{n}$.
3. *Si* $a \equiv c \pmod{n}$ *et* $b \equiv d \pmod{n}$, *alors* $ab \equiv cd \pmod{n}$.
4. *Si* $a \equiv b \pmod{n}$, *alors* $a^k \equiv b^k \pmod{n}$ $(\forall k \in \mathbb{N})$.

Preuve

Preuve

1) Si r est le reste de la division eulidienne de a par n, alors $\exists\ !q \in \mathbb{Z}$ tel que $a = qn + r$ et $0 \leq r < n$, ainsi r est le seul entier qui vérifie $r \equiv a \pmod n$ et $0 \leq r < n$.
De même, si r' est le reste de la division eulidienne de b par n, alors r' est le seul entier qui vérifie $r' \equiv b \pmod n$ et $0 \leq r' < n$.
Par suite

$$a \equiv b \pmod n \Leftrightarrow r \equiv r' \pmod n \Leftrightarrow n \mid (r' - r) \Leftrightarrow r' = r \,(car\, 0 \leq r;\ r' < n).$$

Preuve

1) Si r est le reste de la division eulidienne de a par n, alors $\exists\ !q \in \mathbb{Z}$ tel que $a = qn + r$ et $0 \leq r < n$, ainsi r est le seul entier qui vérifie $r \equiv a \pmod n$ et $0 \leq r < n$.
De même, si r' est le reste de la division eulidienne de b par n, alors r' est le seul entier qui vérifie $r' \equiv b \pmod n$ et $0 \leq r' < n$.
Par suite

$$a \equiv b \pmod n \Leftrightarrow r \equiv r' \pmod n \Leftrightarrow n \mid (r' - r) \Leftrightarrow r' = r\, (car\, 0 \leq r;\ r' < n).$$

2) Si $a \equiv c \pmod n$ et $b \equiv d \pmod n$, alors $n \mid (c - a)$ et $n \mid (d - b)$, donc $n \mid (c + d) - (a + b) +$, ainsi $a + b \equiv c + d \pmod n$.

Preuve

1) Si r est le reste de la division eulidienne de a par n, alors $\exists\ !q \in \mathbb{Z}$ tel que $a = qn + r$ et $0 \leq r < n$, ainsi r est le seul entier qui vérifie $r \equiv a \pmod n$ et $0 \leq r < n$.
De même, si r' est le reste de la division eulidienne de b par n, alors r' est le seul entier qui vérifie $r' \equiv b \pmod n$ et $0 \leq r' < n$.
Par suite

$$a \equiv b \pmod n \Leftrightarrow r \equiv r' \pmod n \Leftrightarrow n \mid (r' - r) \Leftrightarrow r' = r\,(car\,0 \leq r;\ r' < n).$$

2) Si $a \equiv c \pmod n$ et $b \equiv d \pmod n$, alors $n \mid (c - a)$ et $n \mid (d - b)$, donc $n \mid (c + d) - (a + b) +$, ainsi $a + b \equiv c + d \pmod n$.
3) Si $a \equiv c \pmod n$ et $b \equiv d \pmod n$. Montrons que $ab \equiv cd \pmod n$.
On a

$$\begin{cases} a \equiv c \bmod n \\ b \equiv d \bmod n \end{cases} \Rightarrow \begin{cases} n \mid (a - c) \\ n \mid (b - d) \end{cases} \Rightarrow \begin{cases} n \mid b(a - c) \\ n \mid c(b - d) \end{cases} \Rightarrow n \mid ab - cd,$$

donc $ab \equiv cd \pmod n$.

Preuve

1) Si r est le reste de la division eulidienne de a par n, alors $\exists\ !q \in \mathbb{Z}$ tel que $a = qn + r$ et $0 \leq r < n$, ainsi r est le seul entier qui vérifie $r \equiv a \pmod{n}$ et $0 \leq r < n$.
De même, si r' est le reste de la division eulidienne de b par n, alors r' est le seul entier qui vérifie $r' \equiv b \pmod{n}$ et $0 \leq r' < n$.
Par suite

$$a \equiv b \pmod{n} \Leftrightarrow r \equiv r' \pmod{n} \Leftrightarrow n \mid (r' - r) \Leftrightarrow r' = r\,(car\,0 \leq r;\ r' < n).$$

2) Si $a \equiv c \pmod{n}$ et $b \equiv d \pmod{n}$, alors $n \mid (c-a)$ et $n \mid (d-b)$, donc $n \mid (c+d) - (a+b)+$, ainsi $a + b \equiv c + d \pmod{n}$.
3) Si $a \equiv c \pmod{n}$ et $b \equiv d \pmod{n}$. Montrons que $ab \equiv cd \pmod{n}$.
On a

$$\begin{cases} a \equiv c \bmod n \\ b \equiv d \bmod n \end{cases} \Rightarrow \begin{cases} n \mid (a-c) \\ n \mid (b-d) \end{cases} \Rightarrow \begin{cases} n \mid b(a-c) \\ n \mid c(b-d) \end{cases} \Rightarrow n \mid ab - cd,$$

donc $ab \equiv cd \pmod{n}$.
4) En appliquant (3), on trouve que :

$$a \equiv b \pmod{n} \Rightarrow a^k \equiv b^k \pmod{n}\ (\forall k \in \mathbb{N}).$$

Théorème

Soient $n \in \mathbb{N}^*$, $a,\ b,\ c \in \mathbb{Z}^*$ *et soit* $d = \mathrm{pgcd}(c,n)$, *alors :*

$$ac \equiv bc \pmod{n} \Leftrightarrow a \equiv b \pmod{\frac{n}{d}}$$

Théorème

Soient $n \in \mathbb{N}^*$, $a,\ b,\ c \in \mathbb{Z}^*$ *et soit* $d = \text{pgcd}(c,n)$, *alors :*

$$ac \equiv bc \pmod{n} \Leftrightarrow a \equiv b \pmod{\frac{n}{d}}$$

Preuve.

$ac \equiv bc \pmod{n} \Longleftrightarrow a \equiv b \pmod{\frac{n}{d}}$ où $d = \text{pgcd}(c,n)$.
On a $ac \equiv bc \bmod n \Rightarrow n \mid (a-b)c \Rightarrow \frac{n}{d} \mid (a-b)\frac{c}{d}$, et comme $\text{pgcd}(\frac{n}{d}, \frac{c}{d}) = 1$, alors d'après Gauss, on trouve que $\frac{n}{d} \mid (a-b)$, ainsi $a \equiv b \pmod{\frac{n}{d}}$.
Inversement, on a :

$$a \equiv b \bmod \frac{n}{d} \Rightarrow \frac{n}{d} \mid (a-b) \Rightarrow n \mid (a-b)d \Rightarrow n \mid (a-b)c \Rightarrow ac \equiv bc \bmod n.$$



Remarque

Soient $m,\ n \in \mathbb{N}^*$, $a,\ b,\ c \in \mathbb{Z}$, *alors :*

1. *Si* $ac \equiv bc \pmod{n}$ *et* $\operatorname{pgcd}(c,n) = 1$, *alors* $a \equiv b \pmod{n}$.
2. *Si* $a \equiv b \pmod{n}$ *et* $m \mid n$, *alors* $a \equiv b \pmod{m}$.

Remarque

Soient $m,\ n \in \mathbb{N}^*$, $a,\ b,\ c \in \mathbb{Z}$, *alors :*

1. *Si* $ac \equiv bc \pmod{n}$ *et* $\text{pgcd}(c,n) = 1$, *alors* $a \equiv b \pmod{n}$.
2. *Si* $a \equiv b \pmod{n}$ *et* $m \mid n$, *alors* $a \equiv b \pmod{m}$.

Définition

Pour $n \in \mathbb{N}^*$ *on définit* $\mathbb{Z}/n\mathbb{Z}$ *comme étant l'ensemble quotient de* $\mathbb{Z}$ *par la relation de congruence modulo* n. *Soit* $a \in \mathbb{Z}$, *alors la classe d'équivalence de* a *pour cette relation est noté par* $\bar{a}$ *et appelé la classe de* a *modulo* n *et on a :*

$$\overline{a} = \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\} = \{a + nk \mid k \in \mathbb{Z}\}.$$

Et on a

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{a} \mid a \in \mathbb{Z}\}.$$

Corollaire

Soit n un entier strictement positif. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est fini de cardinal n et on a :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0},\ \overline{1},\ \overline{2}, \ldots \overline{n-1}\}.$$

Corollaire

Soit n un entier strictement positif. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est fini de cardinal n et on a :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0},\ \overline{1},\ \overline{2}, \ldots \overline{n-1}\}.$$

Preuve.

Soit $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ et soit r le reste de la division euclidienne de a par n, alors $0 \leq r < n$, ainsi $\overline{a} = \overline{r} \in \{\overline{0},\ \overline{1},\ \overline{2}, \ldots \overline{n-1}\}$, ce qui donne que $\mathbb{Z}/n\mathbb{Z} \subseteq \{\overline{0},\ \overline{1},\ \overline{2}, \ldots \overline{n-1}\}$. L'autre inclusion est trivial, ainsi $\mathbb{Z}/n\mathbb{Z} = \{\overline{0},\ \overline{1},\ \overline{2}, \ldots \overline{n-1}\}$. Comme les classe $\overline{0},\ \overline{1},\ \overline{2}, \ldots$ et $\overline{n-1}$ sont deux à deux disjointes, alors l'ensemble $\mathbb{Z}/n\mathbb{Z}$ est fini de cardinal n. □

Proposition

La relation de congruence modulo n est compatible avec l'addition et la multiplication dans $\mathbb{Z}$ c'est-à-dire si $\overline{a} = \overline{a'}$ et $\overline{b} = \overline{b'}$, alors $\overline{a+b} = \overline{a'+b'}$ et $\overline{ab} = \overline{a'b'}$.

Proposition

La relation de congruence modulo n est compatible avec l'addition et la multiplication dans $\mathbb{Z}$ c'est-à-dire si $\overline{a} = \overline{a'}$ et $\overline{b} = \overline{b'}$, alors $\overline{a+b} = \overline{a'+b'}$ et $\overline{ab} = \overline{a'b'}$.

Preuve.

On a $\overline{a} = \overline{a'}$ et $\overline{b} = \overline{b'}$, donc $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$, ainsi $(a+b) \equiv (a'+b') \pmod{n}$ et $ab \equiv a'b' \pmod{n}$, ce qui donne $\overline{a+b} = \overline{a'+b'}$ et $\overline{ab} = \overline{a'b'}$. □

Proposition

La relation de congruence modulo n est compatible avec l'addition et la multiplication dans $\mathbb{Z}$ c'est-à-dire si $\overline{a} = \overline{a'}$ et $\overline{b} = \overline{b'}$, alors $\overline{a+b} = \overline{a'+b'}$ et $\overline{ab} = \overline{a'b'}$.

Preuve.

On a $\overline{a} = \overline{a'}$ et $\overline{b} = \overline{b'}$, donc $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$, ainsi $(a+b) \equiv (a'+b') \pmod{n}$ et $ab \equiv a'b' \pmod{n}$, ce qui donne $\overline{a+b} = \overline{a'+b'}$ et $\overline{ab} = \overline{a'b'}$. □

Remarque

L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est muni de deux lois internes notées "+" et "·" définies par :

$$\forall (a,b) \in \mathbb{Z}^2, \ \overline{a+b} = \overline{a} + \overline{b} \text{ et } \overline{ab} = \overline{a} \cdot \overline{b}.$$

Exemple

- $\mathbb{Z}/1\mathbb{Z} = \mathbb{Z}/\mathbb{Z} = \{\overline{0}\}$ *avec* $\overline{0} = \{k \mid k \in \mathbb{Z}\} = \mathbb{Z}$.
- $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}; \overline{1}\}$ *avec* $\overline{0} = \{2k \mid k \in \mathbb{Z}\} = 2\mathbb{Z}$ *et* $\overline{1} = \{2k+1 \mid k \in \mathbb{Z}\} = 2\mathbb{Z}+1$.
- $\mathbb{Z}/3\mathbb{Z} = \{\overline{0}; \overline{1}; \overline{2}\}$ *avec* $\overline{0} = \{3k \mid k \in \mathbb{Z}\} = 3\mathbb{Z}$ *et* $\overline{1} = \{3k+1 \mid k \in \mathbb{Z}\} = 3\mathbb{Z}+1$ *et* $\overline{2} = \{3k+2 \mid k \in \mathbb{Z}\} = 3\mathbb{Z}+2$.
- *Dans* $\mathbb{Z}/n\mathbb{Z}$, *on a* $\overline{n} = \overline{0}$, $\overline{n+1} = \overline{1}$ *et en général* $\overline{n+k} = \overline{k}$ $(\forall k \in \mathbb{Z})$.

Proposition

Soient $n \in \mathbb{N}^*$ *et* $m \in \mathbb{Z}$*, alors :*

$$\text{pgcd}(m,n) = 1 \Longleftrightarrow \exists k \in \mathbb{Z} \text{ tel que } \overline{m} \cdot \overline{k} = \overline{1} \text{ (les classes sont modulo } n).$$

On dit que $\overline{m}$ *est inversible pour la multiplication dans* $\mathbb{Z}/n\mathbb{Z}$ *et* $\overline{k}$ *son inverse dans* $\mathbb{Z}/n\mathbb{Z}$ *qu'on note par* $\overline{m}^{-1}$*.*

Proposition

Soient $n \in \mathbb{N}^*$ et $m \in \mathbb{Z}$, alors :

$$\text{pgcd}(m,n) = 1 \Longleftrightarrow \exists k \in \mathbb{Z} \textit{ tel que } \overline{m} \cdot \overline{k} = \overline{1} \;(\textit{ les classes sont modulo } n).$$

On dit que $\overline{m}$ est inversible pour la multiplication dans $\mathbb{Z}/n\mathbb{Z}$ et $\overline{k}$ son inverse dans $\mathbb{Z}/n\mathbb{Z}$ qu'on note par $\overline{m}^{-1}$.

Preuve.

Si $\text{pgcd}(m,n) = 1$, alors d'après le théorème de Bézout il existe (u,v) dans $\mathbb{Z}^2$ tel que $mu + nv = 1$, d'où $\overline{m} \cdot \overline{u} + \overline{n} \cdot \overline{v} = \overline{1}$, mais $\overline{n} = \overline{0}$, donc $\overline{m} \cdot \overline{u} = \overline{1}$.
Réciproquement, si il existe $k \in \mathbb{Z}$ tel que $\overline{m} \cdot \overline{k} = 1$, alors $mk = 1 + tn$ avec $t \in \mathbb{Z}$, d'où $mk - nt = 1$ avec $(k,t) \in \mathbb{Z}^2$, ainsi d'après le théorème de Bézout on déduit que $\text{pgcd}(m,n) = 1$. □

Problème

"Soient des objets en nombre inconnu. Si on les range par 3 il en reste 2. Si on les range par 5, il en reste 3 et si on les range par 7, il en reste 2. Combien a-t-on d'objets ?"

Problème

"Soient des objets en nombre inconnu. Si on les range par 3 il en reste 2. Si on les range par 5, il en reste 3 et si on les range par 7, il en reste 2. Combien a-t-on d'objets ?"

On attribue ce problème au philosophe chinois Sun-Zi (IIIe siècle) et voici la solution qu'il propose :
"Multiplie le reste de la division par 3, c'est-à -dire 2, par 70, ajoute-lui le produit du reste de la division par 5, c'est-à -dire 3, avec 21 puis ajoute le produit du reste de la division par 7, c'est-à -dire 2 par 15. Tant que le nombre est plus grand que 105, retire 105."

Problème

"Soient des objets en nombre inconnu. Si on les range par 3 il en reste 2. Si on les range par 5, il en reste 3 et si on les range par 7, il en reste 2. Combien a-t-on d'objets ?"

On attribue ce problème au philosophe chinois Sun-Zi (IIIe siècle) et voici la solution qu'il propose :
"Multiplie le reste de la division par 3, c'est-à -dire 2, par 70, ajoute-lui le produit du reste de la division par 5, c'est-à -dire 3, avec 21 puis ajoute le produit du reste de la division par 7, c'est-à -dire 2 par 15. Tant que le nombre est plus grand que 105, retire 105."
Donc, d'après Sun-Zi, on a $2 \times 70 + 3 \times 21 + 2 \times 15 = 233$, tant que $233 > 105$ on retire 105, c'est-à-dire 128, tant que $128 > 105$ on retire 105, c'est-à-dire 23, alors la solution du problème sera $233 - 105 - 105 = 23$.
Ceci est vrai car $23 \equiv 2 \pmod 3$, $23 \equiv 3 \pmod 5$ et $23 \equiv 2 \pmod 7$ (mais il faut signaler que ce problème à une infinité de solution !).

Théorème (Théorème des restes chinois)

Soient n_1, ..., n_p *des entiers supérieurs à 2 deux à deux premiers entre eux, et* $a_1, \ldots, a_p$ *des entiers. Le système d'équations :*

$$(S): \begin{cases} x & \equiv & a_1 \pmod{n_1} \\ \vdots & \vdots & \vdots \\ x & \equiv & a_p \pmod{n_p} \end{cases}$$

admet une unique solution modulo $N = n_1 \times \cdots \times n_p$ *donnée par la formule :*

$$x = \sum_{i=1}^{p} u_k N_k a_k = u_1 N_1 a_1 + \cdots + u_p N_p a_p$$

où $N_i = \frac{N}{n_i}$ *et* $u_i N_i \equiv 1 \pmod{n_i}, \ \forall i \in \{1, \cdots, p\}$.

Preuve.

- **Existence** :
Les entiers n_k étant deux à deux premiers entre eux, il en résulte que pour tout entier $k \in \{1, \cdots, p\}$, N_k et n_k sont premiers entre eux et donc N_k est inversible modulo n_k.

Pour tout $k \in \{1, \cdots, p\}$, soit u_k tel que $u_k N_k \equiv 1 \pmod{n_k}$ et soit $x = \sum_{i=1}^{p} u_k N_k a_k$.

Soit $i \in \{1, \cdots, p\}$ et soit $k \in \{1, \cdots, p\} \setminus \{i\}$, alors $N_i = 0 \pmod{n_k}$,
ainsi $x \equiv u_i N_i a_i \pmod{ni}$ or $u_i N_i = 1 \pmod{n_i}$ par définition de u_i,
donc $x \equiv a_i \pmod{n_i}$ pour tout i, ce qui donne que x est une solution du système (S).

- **Unicité modulo** N :
Soit y une autre solution de (S), alors $\forall\ k \in \{1, \cdots, p\}$, $x - y \equiv 0 \pmod{n_k}$,
c'est-à-dire $\forall\ k \in \{1, \cdots, p\}$, n_k divise $(x - y)$.
Les entiers n_k étant deux à deux premiers entre eux, il en résulte que N divise $(x - y)$, c'est-à-dire $x = y \pmod{N}$. □

Exemple

Revenons au problème de Sun-Zi et soit x *le nombre de ces objets, alors :*

Exemple

Revenons au problème de Sun-Zi et soit x le nombre de ces objets, alors :

$$\begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 3 \pmod 5, \\ x \equiv 2 \pmod 7. \end{cases}$$

Exemple

Revenons au problème de Sun-Zi et soit x *le nombre de ces objets, alors :*

$$\begin{cases} x \equiv 2 \pmod{3}, \\ x \equiv 3 \pmod{5}, \\ x \equiv 2 \pmod{7}. \end{cases}$$

Donc d'après le théorème des restes chinois ce système admet une unique solution modulo $3 \times 5 \times 7 = 105$ *donnée par la formule :*

$$x \equiv (2u_1N_1 + 3u_2N_2 + 2u_3N_3) \pmod{105}$$

où

Exemple

Revenons au problème de Sun-Zi et soit x *le nombre de ces objets, alors :*

$$\begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 3 \pmod 5, \\ x \equiv 2 \pmod 7. \end{cases}$$

Donc d'après le théorème des restes chinois ce système admet une unique solution modulo $3 \times 5 \times 7 = 105$ *donnée par la formule :*

$$x \equiv (2u_1N_1 + 3u_2N_2 + 2u_3N_3) \pmod{105}$$

où $\begin{cases} N_1 = \frac{105}{3} = 35,\ N_2 = \frac{105}{5} = 21,\ N_3 = \frac{105}{7} = 15, \\ 35u_1 \equiv 1 \pmod 3 \Longleftrightarrow \overline{35}\,\overline{u_1} = \overline{1} \Longleftrightarrow \overline{2}\,\overline{u_1} = \overline{1} \Longleftrightarrow \overline{u_1} = \overline{2}(\textit{ modulo } 3), \\ 21u_2 \equiv 1 \pmod 5 \Longleftrightarrow \overline{21}\,\overline{u_2} = \overline{1} \Longleftrightarrow \overline{1}\,\overline{u_2} = \overline{1} \Longleftrightarrow \overline{u_2} = \overline{1}(\textit{ modulo } 5), \\ 15u_3 \equiv 1 \pmod 7 \Longleftrightarrow \overline{15}\,\overline{u_3} = \overline{1} \Longleftrightarrow \overline{1}\,\overline{u_3} = \overline{1} \Longleftrightarrow \overline{u_3} = \overline{1}(\textit{ modulo } 7). \end{cases}$

Ainsi $x \equiv (2 \times 2 \times 35 + 3 \times 1 \times 21 + 2 \times 1 \times 15) \equiv 233 \pmod{105} \equiv 23 \pmod{105}$.
Donc le nombre de ces objets peut être 23, 128, 233, 338,...

Proposition

On considère l'équation diophantienne $(E) : ax + by = c$ *avec* $(a,b) \neq (0,0)$ *et* $d = \mathrm{pgcd}(a,b)$, *alors :*

1. *L'ensemble des solutions* S *de* (E) *est non vide si et seulement si* d *divise* c.
2. *Si* d *divise* c, *alors l'ensemble des solutions de* (E) *est*

$$S = \{(x_0 + kb',\ y_0 - ka') \mid k \in \mathbb{Z}\},$$

   avec (x_0, y_0) *est une solution particulière de l'équation* (E) *et* a' *et* b' *sont tel que* $a = a'd$ *et* $b = b'd$.

Preuve

1. Supposons que $S \neq \emptyset$ et soit $(x_1, y_1) \in S$, alors $ax_1 + by_1 = c$, donc $a'dx_1 + b'dy_1 = c$, d'où $d(a'x + b'y) = c$ c'est-à-dire $d \mid c$.
   Inversement, supposons que $d = \text{pgcd}(a,b)$ divise c, alors $\exists\, c' \in \mathbb{Z}$ tel que $c = dc'$. Puisque $\text{pgcd}(a', b') = 1$, alors, d'après le lemme de Bézout, $\exists (u,v) \in \mathbb{Z}^2$ tel que $a'u + b'v = 1$, donc $dc'(a'u + b'v) = dc' = c$, ainsi $a(c'u) + b(c'v) = c$, ce qui veut dire que $S \neq \emptyset$.
2. Supposons que d divise c, alors $a = da'$, $b = db'$, $\text{pgcd}(a', b') = 1$ et $c = dc'$. Comme $S \neq \emptyset$, alors il existe $(x_0, y_0) \in S$, donc

   $$a'dx_0 + b'dy_0 = c \quad (1).$$

   Soit $(x,y) \in S$, donc

   $$a'dx + b'dy = c \quad (2).$$

   De (1) et (2) on tire

   $$a'(x - x_0) = b'(y_0 - y) \quad (3).$$

   Comme $\text{pgcd}(a', b') = 1$, alors, d'après le lemme de Gauss, on trouve que b' divise $(x - x_0)$, donc il existe $k \in \mathbb{Z}$ tel que $x - x_0 = kb'$ c'est-à-dire il existe $k \in \mathbb{Z}$ tel que $x = x_0 + kb'$ et on remplace x dans (3), on trouve $y = y_0 - ka'$. Comme les couples $(x_0 + kb',\ y_0 - ka')$ sont des solutions de l'équation (E), on déduit que $S = \{(x_0 + kb',\ y_0 - ka') \mid k \in \mathbb{Z}\}$.

Exemple

1. *On résoudre l'équation diophantienne* $(E_1) : 5x - 10y = 3$ *dans* $\mathbb{Z}^2$.

Exemple

1. *On résoudre l'équation diophantienne* $(E_1) : 5x - 10y = 3$ *dans* $\mathbb{Z}^2$.
   On a $\mathrm{pgcd}(5, -10) = 5$ *et* $5 \nmid 3$, *alors l'équation* (E) *n'a aucune solution dans* $\mathbb{Z}^2$.

Exemple

1. *On résoudre l'équation diophantienne* $(E_1): 5x - 10y = 3$ *dans* $\mathbb{Z}^2$.
   On a $\text{pgcd}(5, -10) = 5$ *et* $5 \nmid 3$, *alors l'équation* (E) *n'a aucune solution dans* $\mathbb{Z}^2$.
2. *On résoudre l'équation diophantienne* $(E_2): 6x + 8y = 14$ *dans* $\mathbb{Z}^2$.

Exemple

1. *On résoudre l'équation diophantienne* $(E_1): 5x - 10y = 3$ *dans* $\mathbb{Z}^2$.
   On a $\text{pgcd}(5, -10) = 5$ *et* $5 \nmid 3$, *alors l'équation* (E) *n'a aucune solution dans* $\mathbb{Z}^2$.
2. *On résoudre l'équation diophantienne* $(E_2): 6x + 8y = 14$ *dans* $\mathbb{Z}^2$.
   On a $\text{pgcd}(6, 8) = 2 \mid 14$, *alors l'équation* (E) *est équivalente à* $3x + 4y = 7$ *et elle admet une infinité de solution dans* $\mathbb{Z}^2$.

Exemple

1. *On résoudre l'équation diophantienne* $(E_1) : 5x - 10y = 3$ *dans* $\mathbb{Z}^2$.
   On a $\text{pgcd}(5, -10) = 5$ *et* $5 \nmid 3$, *alors l'équation* (E) *n'a aucune solution dans* $\mathbb{Z}^2$.
2. *On résoudre l'équation diophantienne* $(E_2) : 6x + 8y = 14$ *dans* $\mathbb{Z}^2$.
   On a $\text{pgcd}(6, 8) = 2 \mid 14$, *alors l'équation* (E) *est équivalente à* $3x + 4y = 7$ *et elle admet une infinité de solution dans* $\mathbb{Z}^2$.
   On a $\text{pgcd}(3, 4) = 1$, *donc par le lemme de Bézout* $\exists!(u, v) \in \mathbb{Z}^2$ *tel que* $3u + 4v = 1$, *à savoir* $(u, v) = (3, -2)$, *ainsi (21,-14) est une solution pariculière de* (E), *donc l'ensemble des solutions de* (E) *est*
   $S = \{(21 + 4k,\ -14 - 3k) \mid k \in \mathbb{Z}\}$.

Définition

L'indicatrice d'Euler est la fonction φ*, de l'ensemble* $\mathbb{N}^*$ *dans lui-même, définie par :*

$$\begin{array}{rcccl} \varphi & : & \mathbb{N}^* & \longrightarrow & \mathbb{N}^* \\ & & n & \longmapsto & \operatorname{card}\left(\{m \in \mathbb{N}^* \mid m \leq n \text{ et } \operatorname{pgcd}(m,n) = 1\}\right). \end{array}$$

Pour $n \in \mathbb{N}^*$*,* $\varphi(n)$ *s'appelle indicateur d'Euler de* n*.*

Exemples

1. *On a* $\{m \in \mathbb{N}^* \mid m \leq 6$ *et* $\text{pgcd}(m,6) = 1\} = \{1;\ 5\}$, *donc*

$$\varphi(6) = \text{card}(\{1;\ 5\}) = 2.$$

Exemples

1. *On a* $\{m \in \mathbb{N}^* \mid m \leq 6$ *et* $\text{pgcd}(m,6) = 1\} = \{1;\ 5\}$, *donc*

$$\varphi(6) = \text{card}(\{1;\ 5\}) = 2.$$

2. *On a* $\{m \in \mathbb{N}^* \mid m \leq 5$ *et* $\text{pgcd}(m,5) = 1\} = \{1;2;3;4\}$, *donc*

$$\varphi(5) = \text{card}(\{1;2;3;4\}) = 4.$$

Exemples

1. *On a* $\{m \in \mathbb{N}^* \mid m \leq 6$ *et* $\text{pgcd}(m,6) = 1\} = \{1;\ 5\}$, *donc*
$$\varphi(6) = \text{card}(\{1;\ 5\}) = 2.$$

2. *On a* $\{m \in \mathbb{N}^* \mid m \leq 5$ *et* $\text{pgcd}(m,5) = 1\} = \{1;2;3;4\}$, *donc*
$$\varphi(5) = \text{card}(\{1;2;3;4\}) = 4.$$

3. *On a* $\{m \in \mathbb{N}^* \mid m \leq 1$ *et* $\text{pgcd}(m,1) = 1\} = \{1\}$, *donc* $\varphi(1) = \text{card}(\{1\}) = 1$.

Proposition

Soit $n \in \mathbb{N}^*$*, alors* $\varphi(n)$ *est égal au nombre d'éléments inversibles de* $\mathbb{Z}/n\mathbb{Z}$ *c'est-à-dire de* $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{k} \mid 1 \leq k \leq n \text{ et } \mathrm{pgcd}(k,n) = 1\}$*, donc*

$$\varphi(n) = |\,(\mathbb{Z}/n\mathbb{Z})^\times\,|.$$

Exemples

Déterminons $\varphi(5)$ *et* $\varphi(6)$ *:*

$$\mathbb{Z}/5\mathbb{Z} = \{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4}\} \text{ et } \mathbb{Z}/6\mathbb{Z} = \{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4},\overline{5}\}.$$

Et

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Donc

$$(\mathbb{Z}/5\mathbb{Z})^{\times} = \{\overline{1},\overline{2},\overline{3},\overline{4}\},\ \varphi(5) = 4 \quad \text{et} \quad (\mathbb{Z}/6\mathbb{Z})^{\times} = \{\overline{1},\overline{5}\},\ \varphi(6) = 2.$$

Remarque

1. *Soit* $n \in \mathbb{N}^*$*, alors* $\varphi(n)$ *est égal au nombre de générateurs d'un groupe cyclique d'ordre* n*, en particulier* $\varphi(n)$ *est égal au nombre de générateurs de* $(\mathbb{Z}/n\mathbb{Z}, +)$*.*
2. *Soient* $m, n \in \mathbb{N}^*$ *tel que* $\operatorname{pgcd}(m, n) = 1$ *et* $a, b \in \mathbb{Z}$*, alors :*

$$a \equiv b \pmod{mn} \Leftrightarrow a \equiv b \pmod{m} \text{ et } a \equiv b \pmod{n}.$$

Proposition

La fonction φ *est multiplicative c'est-à-dire* $\forall (m,n) \in {\mathbb{N}^*}^2$ *tel que* $\mathrm{pgcd}(m,n) = 1$, *on a*

$$\varphi(mn) = \varphi(m) \times \varphi(n).$$

Preuve

Soit

$$\begin{array}{rccc} \overline{\phi}: & \mathbb{Z}/mn\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}. \\ & \overline{a}^{[mn]} & \mapsto & (\overline{a}^{[m]},\overline{a}^{[n]}) \end{array}$$

On a $\overline{\phi}$ est injectif. En effet, on a

$$\begin{aligned} \overline{\phi}\left(\overline{a}^{[mn]}\right) = \overline{\phi}\left(\overline{b}^{[mn]}\right) &\Rightarrow (\overline{a}^{[m]},\overline{a}^{[n]}) = (\overline{b}^{[m]},\overline{b}^{[n]}) \Rightarrow \begin{cases} \overline{a}^{[m]} = \overline{b}^{[m]} \\ \overline{a}^{[n]} = \overline{b}^{[n]} \end{cases} \\ &\Rightarrow \begin{cases} a \equiv b \pmod{m} \\ a \equiv b \pmod{n} \end{cases} \Rightarrow a \equiv b \pmod{mn} \\ &\Rightarrow \overline{a}^{[mn]} = \overline{b}^{[mn]}. \end{aligned}$$

Comme $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ ont même cardinal, on déduit que $\overline{\phi}$ est une bijection de $\mathbb{Z}/mn\mathbb{Z}$ sur $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$.

On va montrer que $\overline{\phi}$ induit une bijection entre $(\mathbb{Z}/mn\mathbb{Z})^{\times}$ et $(\mathbb{Z}/m\mathbb{Z})^{\times} \times (\mathbb{Z}/n\mathbb{Z})^{\times}$.
Soit $\overline{y}^{[mn]} \in (\mathbb{Z}/mn\mathbb{Z})^{\times}$, on a :

$$\overline{y}^{[mn]} \in (\mathbb{Z}/mn\mathbb{Z})^{\times} \Rightarrow \text{pgcd}(y,mn) = 1 \Rightarrow \text{pgcd}(y,m) = 1 \text{ et } \text{pgcd}(y,n) = 1$$
$$\Rightarrow \overline{y}^{[m]} \in (\mathbb{Z}/m\mathbb{Z})^{\times} \text{ et } \overline{y}^{[n]} \in (\mathbb{Z}/n\mathbb{Z})^{\times}.$$

Soit $(\overline{a}^{[m]}, \overline{b}^{[n]}) \in (\mathbb{Z}/m\mathbb{Z})^{\times} \times (\mathbb{Z}/n\mathbb{Z})^{\times}$, alors $\text{pgcd}(a,m) = 1$ et $\text{pgcd}(b,n) = 1$.
Comme $\overline{\phi}$ est surjectif, il existe $\overline{y}^{[mn]} \in \mathbb{Z}/mn\mathbb{Z}$ tel que $\overline{\phi}(\overline{y}) = (\overline{a}^{[m]}, \overline{b}^{[n]})$, ce qui donne $\overline{y}^{[m]} = \overline{a}^{[m]}$ et $\overline{y}^{[n]} = \overline{b}^{[m]}$, ainsi $\text{pgcd}(y,m) = 1$ et $\text{pgcd}(y,n) = 1$, et comme $\text{pgcd}(m,n) = 1$, alors $\text{pgcd}(y,mn) = 1$, ce qui donne $\overline{y}^{[mn]} \in (\mathbb{Z}/mn\mathbb{Z})^{\times}$. Ainsi $\overline{\phi}$ induit une bijection entre $(\mathbb{Z}/mn\mathbb{Z})^{\times}$ et $(\mathbb{Z}/m\mathbb{Z})^{\times} \times (\mathbb{Z}/n\mathbb{Z})^{\times}$, ce qui donne

$$\varphi(mn) = \varphi(m) \times \varphi(n).$$

Propriétés

1. $\varphi(p) = p-1$ *pour tout nombre premier* p.
2. $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ *pour tout nombre premier* p *et pour tout* $\alpha \in \mathbb{N}^*$.
3. *Si* p *et* q *sont deux nombres premiers différents, alors* $\varphi(pq) = (p-1)(q-1)$.
4. *Si* $n = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ *avec les* p_i *sont des nombres premiers différents et les* α_i *dans* $\mathbb{N}^*$*, alors*

$$\varphi(n) = p_1^{\alpha_1-1} \dots p_s^{\alpha_s-1}(p_1-1)\dots(p_s-1) = n\prod_{i=1}^{s}(1-\frac{1}{p_i}).$$

Preuve

1) On a $\mathrm{card}(\{k \in \mathbb{N}^* \mid k \leq p \text{ et } \mathrm{pgcd}(k,p) = 1\}) = \mathrm{card}(\{1, 2, \ldots, p-1\}) = p - 1$, d'où $\varphi(p) = p - 1$.

Preuve

1) On a $\text{card}(\{k \in \mathbb{N}^* \mid k \leq p \text{ et } \text{pgcd}(k,p) = 1\}) = \text{card}(\{1, 2, \ldots, p-1\}) = p-1$, d'où $\varphi(p) = p - 1$.
2) Soient $p \in \mathbb{P}$ et $\alpha \in \mathbb{N}^*$.
Calculer $\varphi(p^\alpha)$ revient à compter le nombre d'entiers compris entre 1 et p^α (inclus) qui sont premiers avec p^α. Comme p est premier, cela revient à dénombrer le nombre d'entiers de 1 à p^α qui ne sont pas divisibles par p, c'est-à-dire tous les entiers sauf les multiples de p. Or ces multiples de p sont les kp avec $k \in \{1, 2, \ldots, p^{\alpha-1}\}$ qui sont en nombre de $p^{\alpha-1}$ multiples de p, ainsi :

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1).$$

Preuve

1) On a $\text{card}(\{k \in \mathbb{N}^* \mid k \leq p \text{ et } \text{pgcd}(k,p) = 1\}) = \text{card}(\{1,2,\ldots,p-1\}) = p-1$, d'où $\varphi(p) = p-1$.
2) Soient $p \in \mathbb{P}$ et $\alpha \in \mathbb{N}^*$.
Calculer $\varphi(p^\alpha)$ revient à compter le nombre d'entiers compris entre 1 et p^α (inclus) qui sont premiers avec p^α. Comme p est premier, cela revient à dénombrer le nombre d'entiers de 1 à p^α qui ne sont pas divisibles par p, c'est-à-dire tous les entiers sauf les multiples de p. Or ces multiples de p sont les kp avec $k \in \{1,2,\ldots,p^{\alpha-1}\}$ qui sont en nombre de $p^{\alpha-1}$ multiples de p, ainsi :

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1).$$

3) On a $\text{pgcd}(p,q) = 1$ et p et q deux nombres premiers, donc

$$\varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1).$$

4) On a

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{\alpha_1}) \times \varphi(p_2^{\alpha_2} \dots p_s^{\alpha_s}) \\
&= \varphi(p_1^{\alpha_1}) \times \varphi(p_2^{\alpha_2}) \times \varphi(p_3^{\alpha_3} \dots p_s^{\alpha_s}) \\
&= \varphi(p_1^{\alpha_1}) \times \varphi(p_2^{\alpha_2}) \times \varphi(p_3^{\alpha_3}) \dots \times \varphi(p_s^{\alpha_s}) \\
&= p_1^{\alpha_1 - 1}(p_1 - 1) p_2^{\alpha_2 - 1}(p_2 - 1) \dots p_s^{\alpha_s - 1}(p_s - 1) \\
&= p_1^{\alpha_1 - 1} \dots p_s^{\alpha_s - 1}(p_1 - 1) \dots (p_s - 1) \\
&= n \prod_{i=1}^{s} (1 - \frac{1}{p_i}).
\end{aligned}$$

Théorème (Théorème d'Euler)

Soit n un entier naturel non nul, alors

$$(\forall\, a \in \mathbb{Z}) : \ \ \mathrm{pgcd}(a,n) = 1,\ a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Théorème (Théorème d'Euler)

Soit n un entier naturel non nul, alors

$$(\forall\, a \in \mathbb{Z}):\ \ \mathrm{pgcd}(a,n) = 1,\ a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Preuve.

Comme a est inversible modulo n, Il est clair que

$$\{\overline{k} \mid \mathrm{pgcd}(k,n) = 1\} = \{\overline{as} \mid \mathrm{pgcd}(s,n) = 1\},$$

ainsi

$$\prod_{k=1}^{\varphi(n)} \overline{k} = \prod_{s=1}^{\varphi(n)} \overline{as} \Longrightarrow \prod_{k=1}^{\varphi(n)} \overline{k} = \overline{a}^{\varphi(n)} \prod_{s=1}^{\varphi(n)} \overline{s} \Longrightarrow \overline{a}^{\varphi(n)} = 1.$$



Remarque

On peut montrer le théorème d'Euler en utilisant le théorème de Lagrange. En effet, on sait que $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^{\times}$. *Donc, si* $\mathrm{pgcd}(a,n) = 1$ *alors* $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ *et, par le théorème de Lagrange, on tire que*

$$\overline{a}^{\varphi(n)} = \overline{1} \Longleftrightarrow a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Théorème (Petit Théorème de Fermat)

Soit p un nombre premier, alors

$$(\forall\, a \in \mathbb{Z}) : \;\; \mathrm{pgcd}(a,p) = 1,\; a^{p-1} \equiv 1 \pmod{p}.$$

Théorème (Petit Théorème de Fermat)

Soit p un nombre premier, alors

$$(\forall\, a \in \mathbb{Z}) : \;\; \mathrm{pgcd}(a,p) = 1,\, a^{p-1} \equiv 1 \pmod{p}.$$

Preuve.

On a p est premier, donc $\varphi(p) = p - 1$ et d'après le théorème d'Euler on a le résultat.



Théorème (Petit Théorème de Fermat)

Soit p un nombre premier, alors

$$(\forall\, a \in \mathbb{Z}) : \; \text{pgcd}(a,p) = 1,\; a^{p-1} \equiv 1 \pmod{p}.$$

Preuve.

On a p est premier, donc $\varphi(p) = p-1$ et d'après le théorème d'Euler on a le résultat. □

Corollaire

Soit p un nombre premier, alors

$$(\forall\, a \in \mathbb{Z}),\; a^p \equiv a \pmod{p}.$$

En effet, si $\text{pgcd}(p,a) = 1$, alors $a^{p-1} \equiv 1 \pmod{p}$, donc $a^p \equiv a \pmod{p}$. Si p divise a alors $\overline{a} = \overline{0}$ et la propriété est aussi vraie, d'où le résultat.

Théorème (Test de primalité)

Soient $a \in \mathbb{N}^*$, $n \in \mathbb{N}$ *avec* $n \geq 2$. *Si* $a^{n-1} \equiv 1 \pmod{n}$ *et* $a^x \not\equiv 1 \pmod{n}$ *pour tout* x *diviseur strict de* $n-1$, *alors* n *est premier.*

Preuve.

Comme $a^{n-1} \equiv 1 \pmod{n}$, alors $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. L'ordre de $\overline{a}$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$ divise $n-1$, par hypothèse ne peut pas être strictement inférieure à $n-1$, donc égale à $n-1$, d'où $n-1 \leq \varphi(n) < n$.
Si n n'est pas premier, il admettrait un diviseur stricte différent de 1, donc non premier avec n d'où $\varphi(n) < n-1$, ce qui donne une contradiction, ainsi n est premier.



Théorème (Test de primalité)

Soient $a \in \mathbb{N}^*$, $n \in \mathbb{N}$ *avec* $n \geq 2$. *Si* $a^{n-1} \equiv 1 \pmod{n}$ *et* $a^x \not\equiv 1 \pmod{n}$ *pour tout* x *diviseur strict de* $n-1$, *alors* n *est premier.*

Preuve.

Comme $a^{n-1} \equiv 1 \pmod{n}$, alors $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$. L'ordre de $\overline{a}$ dans $(\mathbb{Z}/n\mathbb{Z})^{\times}$ divise $n-1$, par hypothèse ne peut pas être strictement inférieure à $n-1$, donc égale à $n-1$, d'où $n-1 \leq \varphi(n) < n$.
Si n n'est pas premier, il admettrait un diviseur stricte différent de 1, donc non premier avec n d'où $\varphi(n) < n-1$, ce qui donne une contradiction, ainsi n est premier. □

Remarque

Le résultat pour p *premier fut établi par Fermat en* 1640 *(Petit théorème de Fermat) et généralisé ensuite par Euler.*

Proposition

Si p *un nombre premier et* $k \in \{1, 2, \cdots, p-1\}$, *alors* $\binom{p}{k} \equiv 0 \pmod{p}$.

Proposition

Si p un nombre premier et $k \in \{1, 2, \cdots, p-1\}$, alors $\binom{p}{k} \equiv 0 \pmod{p}$.

Preuve.

Dans $\mathbb{Z}/p\mathbb{Z}[X]$, on considère le polynôme $P(X) = (1+X)^p - (1+X)$. Le polynôme P est de degré p, et s'annule sur le corps $\mathbb{Z}/p\mathbb{Z}$, car $a^p \equiv a \pmod{p}$. De même pour le polynôme $Q(X) = X^p - X$. Or ces deux polynômes sont unitaires et de même degré, ils sont donc égaux, donc

$$
\begin{aligned}
P(X) = Q(X) &\Rightarrow X^p + \overline{\binom{p}{p-1}} X^{p-1} + \ldots + \overline{\binom{p}{1}} X - X = X^p - X \\
&\Rightarrow \overline{\binom{p}{p-1}} X^{p-1} + \ldots + \overline{\binom{p}{1}} X = \overline{0} \\
&\Rightarrow \overline{\binom{p}{k}} = \overline{0},\ \forall\, k \in \{1, 2, \cdots, p-1\} \\
&\Rightarrow \binom{p}{k} \equiv 0 \pmod{p},\ \forall\, k \in \{1, 2, \cdots, p-1\}.
\end{aligned}
$$

Fut formulé par Waring en 1770 et démontré par Wilson.

Théorème

1) *Soit p un nombre premier alors $(p-1)! \equiv -1 \pmod{p}$.*
2) *Si un entier $n \geq 2$ vérifié la congruence $(n-1)! \equiv -1 \pmod{n}$, alors n est premier. (Cette assertion présente un autre moyen pour tester la primalité d'un entier).*

Preuve.

1. Il est clair que pour tout élément non nul $x \in \mathbb{Z}/p\mathbb{Z}$ distincts de $\overline{1}$, $\overline{-1}$, on a $x \neq x^{-1}$. En regroupant chaque terme avec son inverse, on obtient que le produit

$$2 \times 3 \times \ldots \times (p-2) \equiv 1 \pmod p.$$

Donc, dans $\mathbb{Z}/p\mathbb{Z}$, on a

$$\overline{(p-1)!} = \overline{(p-1)} = \overline{-1} \Longleftrightarrow (p-1)! \equiv -1 \pmod p.$$

2. Si $1 \times 2 \times \ldots \times (n-1) \equiv -1 \pmod n$, alors les classes $\overline{1}, \overline{2}, \ldots, \overline{n-1}$, sont inversibles dans $\mathbb{Z}/n\mathbb{Z}$. Donc toutes les éléments non nuls de $\mathbb{Z}/n\mathbb{Z}$ sont inversibles, d'où $\mathbb{Z}/n\mathbb{Z}$ est un corps, Par conséquent n est premier.



Proposition

Soit p un nombre premier impair alors

1. *Dans $\mathbb{Z}/p\mathbb{Z}$, il y a $\frac{p+1}{2}$ carrés.*
2. *Si on note par $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$ dans $(\mathbb{Z}/p\mathbb{Z})^*$, alors on a*

$$\left(\frac{x}{p}\right) = \pm\overline{1} \text{ dans } (\mathbb{Z}/p\mathbb{Z})^*.$$

et on a :

$$x \text{ est un carré dans } \mathbb{Z}/p\mathbb{Z} \Longleftrightarrow \left(\frac{x}{p}\right) = \overline{1}.$$

De plus

$$\sum_{x \in (\mathbb{Z}/p\mathbb{Z})^*} \left(\frac{x}{p}\right) = \overline{0} \text{ dans } \mathbb{Z}/p\mathbb{Z}.$$

Preuve

1) On considère l'application

$$f: \begin{array}{ccc} (\mathbb{Z}/p\mathbb{Z})^* & \to & (\mathbb{Z}/p\mathbb{Z})^* \\ x & \mapsto & x^2 \end{array}$$

L'application f est homomorphisme de groupe. Son noyau est constitué par les racines du polynômes $X^2 - \overline{1}$ dans $\mathbb{Z}/p\mathbb{Z}$ c'est-à-dire $\{\pm\overline{1}\}$, donc il est de cardinal 2. On en déduit par le premier théorème d'isomorphisme que

$$\#\mathrm{Im} f = \frac{\#(\mathbb{Z}/p\mathbb{Z})^*}{\#\mathrm{Ker}\, f} = \frac{p-1}{2}.$$

Par conséquent, il y a $\frac{p-1}{2}$ carrés dans $(\mathbb{Z}/p\mathbb{Z})^*$, et puisque $\overline{0}$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$, alors il y en a $\frac{p-1}{2} + 1 = \frac{p+1}{2}$ dans $\mathbb{Z}/p\mathbb{Z}$.

Preuve

2) On se place dans $\mathbb{Z}/p\mathbb{Z}$. Pour tout $a \neq \overline{0}$, on a $\left(a^{(p-1)/2}\right)^2 = a^{p-1} = \overline{1}$ (par le théorème de Fermat), donc $a^{(p-1)/2} \in \mathrm{Ker}\, f = \{\pm\overline{1}\}$ c'est-à-dire $\left(\frac{a}{p}\right) \equiv \pm 1 \pmod{p}$.
D'autre part, remarquons que l'ensemble des racines de $X^{\frac{p-1}{2}} - \overline{1}$ de degré $\frac{p-1}{2}$, contient les $\frac{p-1}{2}$ carrés non nuls de $\mathbb{Z}/p\mathbb{Z}$, donc ils coincident. On conclut que :

$$\begin{aligned} a \text{ est un carré dans } (\mathbb{Z}/p\mathbb{Z})^* &\Longleftrightarrow a \text{ est une racine de } X^{\frac{p-1}{2}} - \overline{1} \\ &\Longleftrightarrow a^{(p-1)/2} \equiv 1 \pmod{p} \\ &\Longleftrightarrow \left(\frac{a}{p}\right) = \overline{1}. \end{aligned}$$

Comme il y a $\frac{p-1}{2}$ carré non nuls et $\frac{p-1}{2}$ non carré, alors

$$\sum_{x \in (\mathbb{Z}/p\mathbb{Z})^*} \left(\frac{x}{p}\right) = \overline{0}$$

se découle facilement.

Corollaire

$-\overline{1}$ *est un carré dans* $\mathbb{Z}/p\mathbb{Z}$ *si et seulement si* $p \equiv 1 \pmod 4$.

Corollaire

$-\overline{1}$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1 \pmod 4$.

Preuve.

On a :

$$\begin{aligned} -\overline{1} \text{ est un carré dans } \mathbb{Z}/p\mathbb{Z} &\iff (-1)^{\frac{p-1}{2}} \equiv 1 \pmod p \\ &\iff \frac{p-1}{2} \text{ est pair} \\ &\iff p \equiv 1 \pmod 4. \end{aligned}$$



Proposition

Soit p *un nombre premier impair divisant* a^2+b^2 *où* a *et* b *sont premiers entre eux, alors* $p \equiv 1 \pmod 4$.

Proposition

Soit p un nombre premier impair divisant a^2+b^2 où a et b sont premiers entre eux, alors $p \equiv 1 \pmod 4$.

Preuve.

Soit p un nombre premier impair divisant a^2+b^2 avec $\mathrm{pgcd}(a,b)=1$, alors $\overline{a}$ ou $\overline{b}$ est non nul dans $\mathbb{Z}/p\mathbb{Z}$ (sinon on aura, d'après Bézout, que $\overline{0}=\overline{1}$. Supposons que $\overline{a} \neq \overline{0}$, alors $\overline{1}+(\overline{a}^{-1})^2\overline{b}^2 = \overline{1}+(\overline{a}^{-1}\overline{b})^2 = \overline{0}$, ce qui entraîne que -1 est un carré modulo p, par conséquent $p \equiv 1 \pmod 4$. □

Proposition

Soit p un nombre premier impair divisant a^2+b^2 où a et b sont premiers entre eux, alors $p \equiv 1 \pmod 4$.

Preuve.

Soit p un nombre premier impair divisant a^2+b^2 avec $\text{pgcd}(a,b)=1$, alors $\overline{a}$ ou $\overline{b}$ est non nul dans $\mathbb{Z}/p\mathbb{Z}$ (sinon on aura, d'après Bézout, que $\overline{0}=\overline{1}$. Supposons que $\overline{a} \neq \overline{0}$, alors $\overline{1}+(\overline{a}^{-1})^2\overline{b}^2 = \overline{1}+(\overline{a}^{-1}\overline{b})^2 = \overline{0}$, ce qui entraîne que -1 est un carré modulo p, par conséquent $p \equiv 1 \pmod 4$. □

Théorème (Théorème des deux carrés de Fermat)

Soit p un nombre premier impair, alors p est la somme de deux carrés parfaits si et seulement si $p \equiv 1 \pmod 4$.